Law Council
OF AUSTRALIA

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

9 March 2021

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2021 Executive as at 1 January 2021 are:

- Dr Jacoba Brasch QC, President
- Mr Tass Liveris, President-elect
- Mr Ross Drinnan, Treasurer
- Mr Luke Murphy, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Chief Executive Officer of the Law Council is Mr Michael Tidball. The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council gratefully acknowledges the contribution of its National Criminal Law Committee to this submission.

Executive Summary

1. The Law Council of Australia is pleased to make this submission to the Parliamentary Joint Committee on Intelligence and Security (**Committee**) review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (**Bill**).

2. The Bill proposes to amend the *Surveillance Devices Act 2004* (Cth) (**SDA**) and *Crimes Act 1914* (Cth) (**Crimes Act**) to confer three new powers on the Australian Federal Police (**AFP**) and Australian Criminal Intelligence Commission (**ACIC**), namely:

   - **data disruption warrants**, which authorise the exercise of 'offensive' data disruption powers to frustrate the suspected commission of an offence using a computer that is punishable by a maximum penalty of three or more years' imprisonment. These warrants can also be accompanied by compulsory assistance orders, which require any person with relevant knowledge or expertise to assist the AFP or ACIC, under penalty of 10 years' imprisonment;
   - **network activity warrants**, which enable the ACIC or AFP to monitor the computer-related activities of criminal groups for the purpose of collecting intelligence, rather than investigating an offence to obtain admissible evidence; and
   - **account takeover warrants**, which authorise the AFP or ACIC to assume control of an online account that is suspected of being used in the commission of an offence punishable by at least three years' imprisonment, to enable an investigation.

3. The Bill also proposes to expand the oversight remit of the Inspector-General of Intelligence and Security (**IGIS**) to cover the actions of the ACIC and AFP under network activity warrants. This requires consideration alongside the proposed amendments to oversight legislation in the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020, which the Committee is reviewing separately.

4. The Law Council acknowledges that law enforcement agencies need powers that are adapted to the specialised context of cyber-enabled offences, particularly serious and harmful offences carried out online, such as child exploitation and terrorism.

5. However, the necessity and proportionality of the proposed powers requires careful scrutiny, both in terms of their overall operational objectives, and their detailed provisions. The new powers represent major expansions of the existing powers of the AFP and ACIC, which depart sharply from the traditional focus of their investigative powers on the collection of admissible evidence of specific offences. They also have the potential to have significant adverse impacts on large numbers of non-suspects who are lawfully using the networks, systems or accounts that are suspected of being used by offenders.

Necessity of the proposed powers

6. As a threshold issue, the Law Council is concerned that the necessity of the proposed powers has not been clearly or adequately established.

7. Most significantly, the Bill proposes to reject a core recommendation of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (**Richardson Review**) that law enforcement agencies should not be conferred with specific cyber-disruption powers in the nature of the proposed data disruption warrant regime. The Law Council considers the reasoning offered for rejecting this recommendation does not directly address the significant principled and practical risks raised by the Richardson Review. In particular, the Richardson Review concluded that there was not a material gap in existing investigative powers, which could justify effectively placing the AFP or ACIC in the position of 'judge, jury and executioner', at the point of determining whether to exercise a power of data disruption that could cause material loss or damage to potentially large numbers of lawful computer users, who are not suspected of any wrongdoing.[1]

8. The Law Council also notes that the supporting justification for the proposal to confer specific intelligence-collection powers on the AFP and ACIC under network activity warrants does not clearly identify a gap in existing powers. In particular:

   - existing provisions of the computer access warrant regime in Division 4 of Part 2 of the SDA already dispense with requirements to establish the identity of an individual computer user, and enable warrants to be issued in relation to a computer that is 'associated with, used by, or likely to be used by, a person (whose identity may or may not be known)';[1]
   - no specific explanation is offered for the proposal to confer intelligence-collection powers on both the AFP and the ACIC, rather than the ACIC alone as the specialist national criminal intelligence agency; and
   - there is no clear acknowledgement of the significant potential for overlap with the existing powers of intelligence agencies, particularly:
     - the security intelligence collection powers of the Australian Security Intelligence Organisation (**ASIO**) in respect of suspected offences that also fall within the statutory definition of 'security' in the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**). Such overlap is especially likely with respect to foreign interference and terrorism; and
     - the powers of the Australian Signals Directorate (**ASD**) to collect intelligence relevant to cybercrime outside Australia, and to disrupt cybercrime outside Australia under section 7 of the *Intelligence Services Act 2001* (Cth) (**ISA**).

9. Similarly, no clear justification is provided for specific powers of 'lockout' from online accounts for the purpose of collecting evidence of an offence, on top of existing computer access and data surveillance powers, which already enable the covert monitoring of a person's activities using those accounts.

Proportionality of the proposed powers

10. The Law Council is further concerned that the proposed scope of the new powers is disproportionately broad compared to the threats of serious and organised cybercrime to which they are directed. It is essential that the public has a credible basis upon which to be satisfied that these powers can only be exercised in relation to the most serious forms of criminality that pose a high risk to public safety, consistent with the stated policy intent.

11. If the Committee considers that the proposed powers are necessary, the Law Council recommends 57 improvements to the Bill (listed below), which principally seek to ensure their proportionality. These recommendations are directed to the following key areas:

    - remedying instances of overbreadth in the offences covered by the new warrants (which are offences punishable by a maximum penalty of three or more years' imprisonment, thereby also covering a wide range of offences at the lower end of the range of objective seriousness);
    - strengthening the degree of independence and rigour of the issuing process, primarily by limiting issuing authorities to judges of superior courts, who are appointed in their personal capacities;
    - addressing various issues in the scope and design of the individual powers able to be exercised under the new warrant types, particularly powers to intercept telecommunications, use surveillance devices and remove items from premises. Many of these issues which replicate problems the Law Council has previously identified in equivalent provisions in the computer access warrant regime in Part 2 of the SDA, as enacted by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**).

[1] SDA, paragraph 27A(15)(c) (meaning of 'target computer' for the purpose of computer access warrants).

List of recommendations

Data disruption warrants (Schedule 1) (recs 1-35 of 57)

Recommendation 1—implementation of Richardson Review recommendations

Preferred option

- **Schedule 1 should be omitted from the Bill, and recommendation 162 of the Richardson Review should be implemented in full.**

Alternative (non-preferred option)

- **If there is no appetite to implement recommendation 162 of the Richardson Review, Schedule 1 to the Bill should be amended consistently with the Law Council's recommendation 5 below. This would implement the alternative recommendation of the Richardson Review that data disruption powers should be authorised only by judicial officers, and not members of the AAT.**

Recommendation 2—persons who may apply for data disruption warrants

- **Proposed subsection 27KA(1) of the SDA (item 13 of Schedule 1) should be amended so that the persons who are authorised to apply for a data disruption warrant are those who meet the following requirements:**
  - **the person is a law enforcement officer in relation to the AFP or ACIC (as applicable) within the meaning of section 6A of the SDA; and**
  - **the person holds a position within the AFP or ACIC (as applicable) that is of a minimum, prescribed level of seniority, which should not be any less than an Executive Level 2 under the *Public Service Act 1999* (Cth) or an equivalent rank; and**
  - **the person has been approved, by written instrument made by the AFP Commissioner or ACIC CEO (as applicable) to apply for data disruption warrants (either by class or individually); and**
  - **the relevant agency head must not approve a person under the above requirement, unless satisfied on reasonable grounds that:**
    - **the person holds a supervisory role in the chain of command;**
    - **it is necessary and proportionate for the person to apply for data disruption warrants in the course of their normal duties with the AFP or ACIC (as applicable); and**
    - **the person possesses the requisite skills, knowledge and experience to make warrant applications, and the person has completed all current internal training requirements for making such applications.**

Recommendation 3—'relevant offences' for data disruption warrants

- **Proposed section 27KA of the SDA (Schedule 1, item 13) and subsequent provisions in new Division 5 of Part 2 should be amended to make the**

following changes to the offences which are eligible for a data disruption warrant:

- **omit the concept of a 'relevant offence' within the meaning of section 6 of the SDA; and**
- **replace it with the approach specified at paragraphs [77]-[78] of this submission.**

Recommendation 4—stronger issuing criteria regarding necessity and proportionality

- **Proposed section 27KC of the SDA (item 13 of Schedule 1) should be amended as follows:**
  - **paragraph 27KC(1)(b) should be amended to omit the reference to the issuance of the warrant being 'justified'. This should be substituted with a requirement that the issuance of the warrant must be 'reasonably necessary' to frustrate the commission of the offence(s) referred to in the warrant application; and**
  - **subsection 27KC(2) should include an additional mandatory consideration in applying the proportionality test. The issuing authority should be required to consider:**
    - **the specific nature of the proposed disruption activities to be carried out under the warrant;**
    - **the proportionality of those activities to the suspected offending;**
    - **the potential adverse impacts on non-suspects; and**
    - **the steps proposed to be taken to avoid or minimise those adverse impacts, and their likely prospects of success.**

Recommendation 5—superior court judges as sole issuing authorities for data disruption warrants

- **Proposed subsection 27KA(2) of the SDA and related provisions of Schedule 1 to the Bill should be amended to provide that the issuing authority for a data disruption warrant is a judge of a superior court of record (specifically, a judge of a State or Territory Supreme Court or the Federal Court of Australia) who is appointed by the Attorney-General in their personal capacity.**

Recommendation 6—an 'investigatory powers division' of the AAT to issue data disruption warrants

- **In the alternative to implementing the Law Council's recommendation 5 above, consideration should be given to implementing recommendations of the third INSLM in his review of the TOLA Act to establish an Investigatory Powers Division of the AAT, headed by a retired superior judge.**

- **If the new Investigatory Powers Division is established, it should also be conferred with powers to issue data disruption warrants.**
- **Consistent with recommendations of the Law Council to the Committee's review of the TOLA Act, there should also be specific statutory eligibility criteria, and a transparent selection process, for all appointments to the new Investigatory Powers Division. The Law Council recommends that these members are superior court judges, who are appointed, in their personal capacities, as members of the new Division for the purpose of issuing warrants.**

Recommendation 7—public interest advocates to act as contradictors in data disruption warrant applications

- **Schedule 1 to the Bill should be amended to establish a regime of public interest advocates to act as contradictors in all applications for data disruption warrants.**
- **The eligibility requirements for appointment as a public interest advocate should be identical to those recommended by the Committee in its August 2020 press freedoms inquiry report (recommendation 2).**

Recommendation 8—statutory definitions of 'disruption' of data and 'frustration' of the commission of an offence

Preferred option

- **Schedule 1 to the Bill should be amended to insert definitions of the concept of 'disrupt' (in relation to data) and 'frustrate' (in relation to the commission of an offence) for the purpose of the proposed data disruption warrant regime. Such definitions could be drafted on an inclusive basis, if necessary.**
- **Amendments to the Bill should be circulated before the Bill is scheduled for debate. The Committee should be requested to review and report to Parliament on those amendments prior to any debate.**

Alternative (non-preferred) option

- **Proposed paragraph 27KA(3)(b) (item 13 of Schedule 1) should be amended to provide that the statement of facts and grounds accompanying all applications for data disruption warrants must specify the following matters:**
  - **the acts or types of acts of data disruption that are proposed to be carried out under the warrant;**
  - **the anticipated impacts of those specific acts or types of acts of disruption on the commission of the relevant offence (that is, how they are intended to frustrate that offence); and**
  - **the likelihood that the relevant acts or types of acts of disruption will achieve that objective.**

Recommendation 9—removal or limitation of authority to cause material loss or damage to third-party, lawful computer users

Preferred option

- **In the absence of evidence justifying the necessity of proposed paragraph 27KE(7)(b) (item 13 of Schedule 1), this provision should be omitted from the Bill.**
- **It should be substituted with an absolute prohibition on the AFP and ACIC doing acts or things that are likely to cause material loss or damage to third-party computer users, who are not suspects or persons of interest in an investigation or operation.**

Alternative (non-preferred option)

- **If the Committee is satisfied that data disruption warrants should authorise the AFP and ACIC to do acts or things that are likely to cause material loss or damage to non-suspects who are lawfully using computers, the Bill should be amended as follows, in addition to implementation of the Law Council's previous recommendations:**
  - **the authorisation conferred under proposed paragraph 27KE(7)(b) should be subject to a higher threshold, being that of necessity (not merely 'justified and proportionate');**
  - **the authorisation conferred under proposed paragraph 27KE(7)(b) should be limited to acts of data disruption done under the warrant, and acts that are directly preparatory or incidental to data disruption. It should not apply to any or all of the acts or things authorised under the warrant (such as entry to premises, access to data, or the temporary removal of computers or things from premises);**
  - **the AFP and ACIC should be subject to specific obligations to provide particulars in their warrant applications about:**
    - **the likely impacts of all acts done under the warrant on non-suspects who are lawfully using a computer;**
    - **the steps that will be taken to avoid or minimise those impacts; and**
    - **the likely effectiveness of those steps in avoiding or minimising the likely impacts on non-suspects.**
  - **the AFP and ACIC should be required to notify the Commonwealth Ombudsman if any acts or things are done in purported reliance on a data disruption warrant, which are likely to cause material loss or damage to third-party computer users. Notification must be given as soon as possible after the AFP or ACIC becomes aware of the likely impacts on third parties;**
  - **the AFP and ACIC should be required to include information in their annual reports (at least on a classified basis) about the circumstances in which they have relied on the authority of proposed paragraph 27KE(7)(b) to engage in activities which are likely to cause material loss or damage to non-suspects; and**

- **the Bill should also make consequential amendments to Division 476 of the Criminal Code and section 14 of the ISA, to ensure that:**
  - **ASD staff members are treated identically to AFP, ACIC and ASIO officials under subsection 476.2(4) of the Criminal Code, when ASD staff members are executing data disruption warrants for the AFP or ACIC. (That is, these staff members will have lawful authority, and therefore immunity, when acting within the limits of authority under a data disruption warrant); and**
  - **the broader immunity in section 476.5 of the Criminal Code, which could potentially cover acts of ASD staff members that exceeded the limits of authority under a data disruption warrant, will not apply to the actions of ASD staff members in executing data disruption warrants.**

Recommendation 10—scope of telecommunications interception power

- **The telecommunications interception power in proposed subsection 27KE(2)(h) of the SDA (Schedule 1, item 13) should be amended so that it can only be exercised:**
  - **for the purpose of a sub-set of the activities in proposed subsection 27KE(2) that may be authorised under a disruption warrant. In particular, interception should be limited to accessing data and performing disruption activities. Interception should not be permitted for the purpose of entering or exiting premises under a disruption warrant; and**
  - **if it is <u>necessary</u> to intercept a telecommunication for the purpose of doing one or more of those activities.**
- **Equivalent amendments should be made to the computer access warrant provisions in paragraph 27E(2)(h) of the SDA and paragraph 25A(4)(ba) of the ASIO Act.**

Recommendation 11—scope of power to use force against persons and things

- **The power to use force against persons or things in proposed paragraph 27KE(8)(a) of the SDA (Schedule 1, item 13) should be amended as follows:**
  - **the issuing authority should have discretion to authorise the use of force under each warrant, as is the case for the other activities specified in proposed subsection 27KE(2);**
  - **the statutory power to use force against persons or things should only be conferred for the purpose of entering or exiting premises, where that is authorised under proposed paragraphs 27KE(2)(a) and (b); and**
  - **the statutory power to use force against persons or things should be limited to particular persons or classes of persons (being police officers, or others who have been specifically trained and**

accredited in the use of force) and not any person who exercises authority under a warrant.

- **Equivalent amendments should be made to existing paragraph 27E(6)(a) of the SDA and existing paragraph 25A(5A)(a) of the ASIO Act, which authorise the use of force against persons and things under computer access warrants.**

Recommendation 12 —statutory safeguards on powers to temporarily remove computers and other things from premises

- **The power to temporarily remove computers and other things from premises in proposed paragraph 27KE(2)(f) and subsection 27KE(3) (item 13 of Schedule 1) should be amended as follows:**
  - **the AFP and ACIC should be subject to an explicit timeframe to return a computer or other thing that is removed from premises. They should be required to obtain a further warrant to retain the computer or other thing for any longer period, including after the warrant ceases to be in force;**
  - **the 'other things' which can be removed from premises should be limited to data storage devices and other peripheral items for the operation of a computer, and only for the purpose of accessing or manipulating data, or performing data disruption activities under paragraphs 27KE(2)(c)-(e) and (g); and**
  - **the removal of a computer or another thing from warrant premises should be subject to an explicit threshold of necessity and proportionality.**

Recommendation 13—statutory safeguards for post-warrant concealment powers

- **The powers of post-warrant concealment in proposed subsection 27KE(9) should be amended as follows:**
  - **the matters in the Law Council's recommendations 8-12 in relation to proposed subsection 27KE(2) should be applied equally to the corresponding concealment powers in proposed subsection 27KE(9); and**
  - **the power to undertake a post-warrant concealment activity more than 28 days after the warrant has expired should require separate, external authorisation by an issuing authority, consistent with the recommendations of the third INSLM in relation to computer access warrants.**
- **The corresponding post-warrant concealment powers for computer access warrants in subsection 27E(7) of the SDA and subsection 25A(8) of the ASIO Act should also be amended accordingly.**

Recommendation 14—limitations on extensions of data disruption warrants

- **Proposed subsections 27KD(2) and 27KF(1) (item 13 of Schedule 1) should be amended to provide that the total maximum duration of a data**

disruption warrant is 90 days, inclusive of any extensions if the warrant is initially issued for a period of less than 90 days.

- **If the AFP or ACIC consider that there is a need to carry out further data disruption activities after the 90-day total maximum period of effect for a data disruption warrant, then they should be required to seek a new warrant.**

Recommendation 15— no extraterritorial application of data disruption warrants

- **The Bill should be amended to omit proposed section 43C of the SDA (Schedule 1, item 27).**
- **Rather than data disruption warrants having extraterritorial application, ASD should have exclusive responsibility for undertaking activities outside Australia to prevent and disrupt cyber-enabled crime, pursuant to paragraph 7(1)(c) of the ISA.**

Recommendation 16—no emergency authorisations for data disruption powers

- **The Bill should be amended to omit the proposed amendments to Part 3 of the SDA (items 15-24 of Schedule 1). Data disruption powers should not be subject to the regime of emergency authorisations.**
- **If there is a need for the expedited approval of data disruption powers in time critical circumstances, then it should be addressed through practical mechanisms to enable the making and determination of warrant applications in urgent cases.**
- **Consideration could be given to legislative amendments to create a discrete regime for requesting and issuing emergency warrants. However, this course should be taken only if it is established that the general provisions governing warrant applications and issuing decisions would not operate effectively in urgent cases.**

Recommendation 17—'last resort threshold' for emergency authorisations

- **If emergency authorisations are to be available for data disruption, contrary to the Law Council's primary recommendation above, then proposed section 28(1C) of the SDA (item 15 of Schedule 1) should be amended as follows**:
  - **proposed paragraph 28(1C)(c) should be replaced with a requirement for the authorising officer to be satisfied, on reasonable grounds, that there are no alternative means available to prevent or minimise the causation of serious violence or substantial property damage that are likely to be as effective as data disruption, in the particular factual circumstances; and**
  - **the authorising officer should also be required to consider the likely impacts of the proposed data disruption activity on third parties who are using, or are reliant on, the target computer. The authorising officer should only be able to grant the emergency authorisation if satisfied, on reasonable grounds, that:**

- **adequate arrangements are in place to minimise, to the greatest possible extent, those impacts; and**
- **any likely impacts on third parties are proportionate to the objective of the emergency authorisation, to prevent or mitigate serious, imminent violence or property damage**.

Recommendation 18—orders if an emergency authorisation for data disruption powers is not approved

- **If emergency authorisations are to be available for data disruption, contrary to the Law Council's primary recommendation above, then proposed section 35B (item 23 of Schedule 1) should be amended to confer the following powers on an issuing authority, if they decline to retrospectively approve an emergency data disruption authorisation:**
  - **the issuing authority may require the AFP or ACIC to disclose the existence of the data disruption activity to an owner, operator or user of a computer or data, who has been adversely affected by the disruption activity. This should be subject to a requirement to be satisfied that such disclosure is not likely to cause serious prejudice to law enforcement operations or capabilities or national security; and**
  - **the issuing authority may require the AFP or ACIC to take such remedial action as considered appropriate in the circumstances, including, but not limited to, financial compensation.**

Recommendation 19—'appropriate authorising officers' for the ACIC for emergency authorisations concerning data disruption

- **If emergency authorisations are to be available for data disruption, contrary to the Law Council's primary recommendation above, then the Bill should be amended to provide that the following persons are authorised to issue emergency data disruption warrants for the ACIC:**
  - **the CEO of the ACIC; and**
  - **a Senior Executive Service-level employee of the ACIC, who has been authorised in writing by the CEO to issue emergency authorisations for data disruption.**

Recommendation 20—enhancements to statutory notification requirements for data disruption warrants

- **The requirements to notify the Ombudsman of certain acts or things done under data disruption warrants should be amended as follows:**
  - **the notification requirement in proposed section 49C (item 41 of Schedule 1 to the Bill) should be expanded to cover concealment-related actions carried out under proposed subsection 27KE(9) while a data disruption warrant is in force, and up to 28 days after it expires; and**
  - **a new provision should be inserted in Division 2 of Part 6 of the SDA, equivalent to existing section 49B in relation to computer**

access warrants. It should require the AFP and ACIC to notify the Ombudsman of any post-warrant concealment acts carried out under proposed subsection 27KE(9) more than 28 days after a warrant has ceased to be in force.

Recommendation 21—resourcing for oversight of data disruption warrants (also applicable to network activity and account takeover warrants)

- **The Government should increase the budget of the Commonwealth Ombudsman, to enable the effective oversight of the new powers conferred by the Bill, including data disruption. Additional resourcing should enable the Ombudsman to:**
  - **have an appropriate number of security-cleared staff to perform inspection, investigatory and complaints handling functions;**
  - **have appropriate security infrastructure, including accredited premises and ICT systems for information of the highest national security classification that is likely to be generated under all of the new warrant regimes proposed in the Bill; and**
  - **access independent technical expertise, to enable effective oversight of the proposed powers, and existing electronic surveillance powers within the Ombudsman's remit.**

Recommendation 22—expansion of Ombudsman's inspection functions concerning data disruption warrants (also relevant to other proposed warrant types)

- **The Ombudsman's inspection functions in relation to the new powers proposed in the Bill, including data disruption, should be expanded to cover matters additional to agencies' compliance with the SDA.**
- **The expanded inspection functions in relation to the AFP and ACIC should be akin to the broader oversight remit of the IGIS in relation to intelligence agencies, under section 8 of the IGIS Act.**

  In particular, it should cover:
  - **agencies' compliance with applicable policies and procedures (as well as the provisions of the SDA and related legislation);**
  - **the propriety of agencies' actions, practices and policies under the new warrant-based regimes; and**
  - **the compatibility of agencies' actions, practices and policies under the new warrant-based regimes with Australia's international human rights obligations.**

Recommendation 23—removal of Attorney-General's information certification power in the Ombudsman Act, in relation to oversight of data disruption warrants

- **The Ombudsman Act should be amended so that the Attorney-General's certification power in subsection 9(3) cannot be invoked to prevent the provision of information to the Ombudsman for the purpose of performing any oversight function in relation to data disruption warrants or emergency authorisations for data disruption.**

Recommendation 24—oversight of ASD's activities under data disruption warrants

- **The IGIS Act should be amended to provide that, for the avoidance of any doubt, staff members of ASD are subject to IGIS oversight if they are seconded to the AFP or ACIC to execute a data disruption warrant for and on behalf of the AFP or ACIC (as applicable).**

Recommendation 25—additional Ministerial reporting requirements

- **Proposed subsection 49(2D) of the SDA (item 40 of Schedule 1) should be amended to make provision for the following matters:**
  - **the reports of the AFP and ACIC to the Minster on each data disruption warrant must include the additional content listed at paragraph [307] of this submission; and**
  - **the AFP and ACIC must give the Minister a separate report on post-warrant concealment activities carried out under proposed subsection 27KE(9) if any such activities are carried out after a warrant report has been given to the Minister under proposed subsection 49(2D) of the SDA.**

Recommendation 26—additional annual reporting requirements

- **Section 50 of the SDA (as amended by items 41-42 of Schedule 1) should be amended to require annual reports on data disruption warrants to provide aggregated statistical information on the matters identified in paragraph [307] of this submission, in relation to all data disruption warrants issued during the relevant financial year.**

Recommendation 27—specific exclusionary rule of evidence for information obtained under data disruption warrants

<u>Preferred option</u>

- **Proposed section 65C of the SDA (item 51 of Schedule 1) should be omitted from the Bill and replaced with a provision stating that information obtained from the execution of a data disruption warrant is not admissible in criminal proceedings against a person for the relevant offence or relevant offences specified in the data disruption warrant.**

<u>Alternative (non-preferred) option</u>

- **If the Law Council's primary recommendation is not implemented:**
  - **the Government should provide the Committee with information about the arrangements for the training, authorisation and supervision of ASD staff members to execute data disruption warrants, in the context of collecting admissible evidence;**
  - **A staff member of ASD should not be made available to the AFP or ACIC, in any capacity, unless they have satisfactorily completed**

the above training and have complied with periodic re-accreditation requirements;

- **the IGIS and Ombudsman should incorporate the matter of training and supervision of ASD staff members in the context of evidence collection activities into their respective agency inspection plans for ASD, the AFP and ACIC under the data disruption warrant regime;**
- **proposed section 47B of the SDA (item 39 of Schedule 1) should be omitted from the Bill; and**
- **there should be an independent review of the operation of proposed section 65C of the SDA, and the use of evidence obtained pursuant to data disruption warrants, after an appropriate period of time (indicatively, around three years after the commencement of proposed section 65C).**

Recommendation 28—permitted disclosures in relation to legal advice about a warrant issued under the SDA (including data disruption warrants)

- **The Bill should further amend section 45 of the SDA to insert a permitted purpose for the disclosure of protected information (and preparatory dealings with that information). This should cover disclosures for the purpose of obtaining legal advice, or initiating legal proceedings, in connection with a warrant or emergency authorisation, or acts done under the warrant or emergency authorisation.**
- **This new ground of 'permitted disclosure' should apply to <u>all types</u> of warrants and emergency authorisations under the SDA. However, as an absolute minimum, it should cover data disruption warrants and emergency authorisations for data disruption.**

Recommendation 29—removal of power to compel assistance for data disruption

- **The Bill should be amended to provide that mandatory assistance orders under proposed section 64B of the SDA (item 47 of Schedule 1) cannot compel a person to carry out acts of data disruption, which are authorised by a data disruption warrant or an emergency authorisation for data disruption.**

Recommendation 30—issuing authorities and issuing process for mandatory assistance orders in relation to data disruption warrants

- **Proposed section 64B of the SDA (item 47 of Schedule 1) should be amended as follows:**
  - **only superior court judges (appointed in their personal capacity) should be able to issue a mandatory assistance order, consistent with the Law Council's recommendations on disruption warrants;**
  - **applications for such orders should be conducted *inter partes*, unless a prescribed exception exists, on the grounds of urgency, or risks of prejudice to an operation or safety and security; and**

- **if an application is conducted on an e*x parte* basis, public interest advocates, as recommended above in relation to disruption warrants, should be appointed to act as contradictors.**

Recommendation 31—issuing criteria for mandatory assistance orders in relation to data disruption warrants

- **If compulsory assistance orders are to be available in respect of data disruption warrants or emergency authorisations, then the issuing criteria in proposed paragraph 64B(2)(a) of the SDA (item 47 of Schedule 1) should be amended. An issuing authority should only be able to make an order if satisfied, on reasonable grounds, of the following matters:**
  - **compelling a person to carry out an act of data disruption is <u>necessary</u> to frustrate the commission of the relevant offence or offences that are covered by the data disruption warrant; and**
  - **the compulsion of that assistance is justifiable and proportionate, having regard to the relevant offences <u>as well as</u> the likely impacts of the data disruption activity on:**
    - **the person who is subject to the order, and any related parties (such as their employer, or the entity to whom the person is providing services under a contract); and**
    - **other persons, including lawful computer users or clients of the person subject to the order, who may be adversely affected by the data disruption activity.**

Recommendation 32—content and form requirements for all mandatory assistance orders relevant to data disruption warrants

- **Proposed section 64B of the SDA (item 47 of Schedule 1) should be amended to impose the requirements set out at paragraphs [381]-[383] of this submission, with respect to:**
  - **a statutory maximum period of effect for orders, during which time they must be served and executed, or will lapse if this does not occur;**
  - **a prohibition on a single compulsory assistance order purporting to compel the repetitive provision of a specified act of assistance on multiple occasions over a period of time; and**
  - **requirements in relation to:**
    - **the form in which orders and applications must be made (namely, in writing);**
    - **the inclusion of key particulars in all orders (including specification of a compliance period or deadline); and**
    - **obligations for service of orders on the specified person (with the commencement of an order and compliance timeframes tied to the date and time of service).**

Recommendation 33—implementation of third INSLM recommendations about mandatory assistance orders

- **Proposed section 64B of the SDA (item 47 of Schedule 1) should be amended to:**
  - **implement the recommendations of the third INSLM about mandatory assistance orders under section 64A of the SDA and section 3LA of the Crimes Act. Namely, there should be an express provision prohibiting a mandatory assistance order from authorising, or being executed in a manner that amounts to, the detention of a person; and**
  - **impose a related obligation on the AFP Commissioner and ACIC CEO, to take ensure that their agencies have implemented adequate arrangements to enable their compliance with this prohibition in executing all mandatory assistance orders.**

Recommendation 34—Ombudsman oversight of mandatory assistance orders

- **Proposed section 49C of the SDA (item 41 of Schedule 1) should be amended, or an equivalent provision inserted, to require the AFP and ACIC to notify the Ombudsman of the execution of a compulsory assistance order issued under proposed section 64B, in addition to requirements to provide notification about acts or things done under a data disruption warrant.**
- **The Ombudsman's inspection powers in Division 3 of Part 6 of the SDA should be amended to confer an express, discretionary power on the Ombudsman (and staff) to enter premises and be present during the execution of a mandatory assistance order issued under proposed section 64B, which compels a person to attend a specified place to render the assistance sought.**

Recommendation 35—enhanced record-keeping and reporting requirements for mandatory assistance orders

- **The Bill should be amended to:**
  - **extend the Ministerial reporting requirements in section 49 of the SDA, and annual reporting requirements in section 50 of the SDA, to cover mandatory assistance orders issued in relation to warrants or emergency authorisations; and**
  - **require the register of warrants and emergency authorisations under section 53 of the SDA to include details of any mandatory assistance orders issued in respect of each warrant or emergency authorisation.**

Network activity warrants (Schedule 2) (recs 36-40 of 57)

Recommendation 36—common issues with other warrant types

- **The Law Council's recommendations 3, 5-7, 10, 11-13, 15-19, 24, 28-33 in relation to the proposed data disruption warrant regime should also be**

implemented with respect to equivalent provisions in the proposed network activity warrant regime.

Recommendation 37—definition of a 'criminal network of individuals'

- **The following amendments should be made to Schedule 2 to the Bill:**
  - **The definition of a 'criminal network of individuals' in proposed section 7A of the SDA (item 8 of Schedule 1 to the Bill) should be amended to require there to be a reasonable suspicion of a nexus between:**
    - **the suspected conduct of an individual group member in committing an offence, or facilitating the commission of an offence (or having done so, or being likely to do so); and**
    - **the actions or intentions of the group as a whole.**

    (That is, there should be a requirement to establish that the group as a whole was pursuing a common criminal purpose, and the conduct of the individual member or members was directed to that common criminal purpose.)
  - **The requirements in proposed paragraph 27KK(1)(b) (item 9 of Schedule 2 to the Bill) should also be amended to require proof that access to data held in the target computer is likely to substantially assist in the collection of intelligence that:**
    - **relates to the group, or the actions of one or more of its individual members <u>in pursuit of a common criminal purpose of the group</u>; and**
    - **is relevant to the prevention, detection or frustration of one or more kinds of relevant offences, <u>which are committed or facilitated in pursuit of a common criminal purpose of the group (or are likely to be so committed or facilitated).</u>**

Recommendation 38—power to authorise the use of surveillance devices under network activity warrants

<u>Preferred option</u>

- **The Bill should be amended to omit the power to use surveillance devices under a network activity warrant, in proposed paragraph 27KP(2)(i) of the SDA (item 9 of Schedule 2 to the Bill).**
- **The corresponding concealment power in proposed paragraph 27KP(8)(i) should also be omitted.**

<u>Alternative (non-preferred) option</u>

- **If network activity warrants are to be capable of authorising the use of a surveillance device, proposed paragraph 27KP(2)(i) should be amended so that the issuing authority is required to specifically approve the following matters:**
  - **the activities under proposed section 27KP(2) for which a surveillance device may be used; and**

- **the specific type or types surveillance devices that may be used for those activities.**

- **The power to use surveillance devices for the purposes of concealment under proposed paragraph 27KP(8)(i) should be similarly limited to the activities and purposes that were approved under proposed paragraph 27KP(2)(i).**

Recommendation 39—oversight of network activity warrants

- **The Government should ensure that the budget of the IGIS is increased as necessary to ensure that there is no reduction in current levels of oversight as a result of the expansion of its functions, including in relation to network activity warrants.**
- **Further consideration should be given to mechanisms to ensure that a single operation by the AFP into cyber-enabled crime is subject to consistent and comprehensive oversight, irrespective of the particular oversight body responsible for different warrant types. In particular, consideration should be given to:**
  - **revising the proposal to only invest the IGIS with oversight functions in relation to the AFP under network activity warrants, and to expand oversight functions to cover all of the AFP's activities that involve the collection, correlation, analysis, production or dissemination of intelligence; or**
  - **expanding the inspection functions of the Ombudsman to include matters of propriety, and to have a similar degree of flexibility in relation to timing and focus as the inspection functions of the IGIS.**

Recommendation 40— re-consideration of the issuing process and thresholds for ASIO computer access warrants, to better align with network activity warrants

- **Further consideration should be given to whether there is a compelling, principled basis for retaining distinctions between the issuing and public reporting requirements for ASIO's computer access warrants, and network activity warrants for the AFP and ACIC, in view of the potential for significant overlap in the subject-matter covered by both warrant types. (That is, where the 'relevant offence' for a network activity warrant also falls within the definition of 'security' in the ASIO Act, as is the case with, for example: terrorism, foreign incisions, foreign interference and espionage offences.)**

Account takeover warrants (Schedule 3) (recs 41-51 of 57)

Recommendation 41—amendments to account takeover warrant regime to address common or similar issues across all three new warrant types

- **The account takeover warrant provisions in proposed Part IAAC of the Crimes Act (Schedule 3 to the Bill) should be amended in line with previous recommendations in this submission concerning data disruption or network activity warrants (or both) with respect to the following matters:**

- **the definition of a 'relevant offence' for the purpose of account takeover warrants should be aligned with the Law Council's recommendation 3 above;**

- **the 'law enforcement officers' of the AFP and ACIC who may apply for account takeover warrants should be limited to staff members of a minimum classification, who have been specifically authorised by the AFP Commissioner or ACIC CEO (as applicable). The statute should not automatically authorise all staff AFP and ACIC members to be applicants;**

- **the issuing authority for account takeover warrants should be a superior court judge, appointed *persona designata*; and**

- **any ability to engage in post-warrant concealment activities more than 28 days after an account takeover warrant has ceased to be in force should require independent authorisation.**

- **The mandatory assistance order regime for account takeover warrants in proposed section 3ZZVG of the Crimes Act (Schedule 3 to the Bill) should be amended in line with equivalent recommendations of the Law Council for other types of assistance orders. In particular:**
  - **The issuing criteria for mandatory assistance orders should require consideration of whether the person is, or has been, the subject of any previous mandatory assistance orders (under multiple regimes);**
  - **there should be an explicit requirement for all mandatory assistance orders to specify material particulars, including the date or time period over which the assistance must be rendered and the nature of the relevant assistance; and**
  - **mandatory assistance orders should be subject to the same reporting and record-keeping obligations as the underlying account takeover warrant.**

Recommendation 42—justification for coercive account takeover powers

- **The proposed account takeover warrant regime in Schedule 3 to the Bill should not proceed unless and until a detailed justification of the perceived necessity is provided publicly, and the Parliament and public have an adequate opportunity to scrutinise it.**
- **This justification should provide specific reasons for the perceived necessity of a power to lock a person out of their account, in addition to existing electronic surveillance powers to monitor the person's activities using that account.**
- **If the objective is to preserve evidence of a suspected 'relevant offence', by preventing its destruction by the account holder or others with access to the account, then this should be explicitly incorporated in the issuing criteria for account takeover warrants.**

Recommendation 43—definition of an 'online account'

- **The definition of an 'online account' and its component term 'electronic service' in proposed section 3ZZUK of the Crimes Act (item 4 of Schedule 3) should be amended to cover a more limited sub-set of online accounts, such as social media, email, and data or voice messaging accounts.**
- **However, if there is no intention to limit the definition of an 'online account' in this way, the issuing criteria for account takeover warrants in proposed section 3ZZUP of the Crimes Act (item 4 of Schedule 3) should apply specific exclusions or limitations in relation to online accounts that are used to provide essential services to a person, such as banking and governmental services.**

Recommendation 44—requirement for affidavits

- **Proposed section 3ZZUN of the Crimes Act (item 4 of Schedule 3) should be amended to require all applications for account takeover warrants to be accompanied by a sworn affidavit, setting out the facts and grounds on which the warrant application is based.**

Recommendation 45—duration of warrants and authorisation of repetitive acts

- **Proposed subsection 3ZZUQ(3) of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to provide that an account takeover warrant must be executed within seven days of its issuance, and automatically ceases to be in force once the AFP or ACIC has gained exclusive control of the account (akin to search warrants).**
- **If the AFP or ACIC seek to re-gain exclusive control of that account if that control is lost for any reason, they should be required to obtain specific authorisation from the issuing authority, ideally under a fresh account takeover warrant.**

Recommendation 46—assessment of third-party impacts

- **Proposed subsection 3ZZUP(2) of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to require the issuing authority to consider whether a proposed account takeover warrant is likely to have adverse impacts on third parties.**
- **This should include specific requirements to assess likely:**
  - **impacts on personal privacy**
  - **financial impacts (on individuals and businesses);**
  - **impacts on a person's ability to conduct their business and personal affairs (including employment or education); and**
  - **impacts on a person's ability to have contact with family members, or provide or receive care.**

Recommendation 47—omission of power to cause loss of, or damage to, data

Preferred option

- **Proposed paragraph 3ZZUR(8)(a) of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to provide that the AFP and ACIC must not execute a warrant in a manner that results in loss of, or damage to, data. There should be no general exception for loss or damage that is considered to be 'justified and proportionate'.**

Alternative (non-preferred) option

- **If the Committee considers there is a compelling justification for authorising the AFP or ACIC to cause loss of, or damage to, data in the course of executing an account takeover warrant, this should be among the powers in proposed subsection 3ZZUR(2) that the issuing authority may individually authorise, if satisfied the applicable issuing threshold is met.**

Recommendation 48—statutory compensation rights

- **Proposed section 3ZZWA of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to extend statutory compensation rights to persons who suffer either direct or indirect loss, damage or injury from the execution of an account takeover warrant.**

Recommendation 49—notification requirement

- **Schedule 3 to the Bill should be amended to:**
  - **require the AFP or ACIC to notify an account holder that their account is the subject of an account takeover warrant; and**
  - **authorise the issuing authority to make an order, on the application of the AFP or ACIC, to either delay or dispense with the notification requirement, if satisfied on reasonable grounds that giving notification to the account holder would frustrate an investigation, or jeopardise the life or safety of any person.**

Recommendation 50—obligation to restore account access

- **Proposed section 3ZZUV of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended, to**
  - **require the AFP and ACIC to take all reasonable steps to restore an account holder's access, after an account takeover warrant has ceased to be in force;**
  - **remove the requirement in proposed paragraph 3ZZUV(b) for the AFP or ACIC to form a view on whether it is lawful for the account holder to operate the account, and replace this with an ability to apply to an issuing authority for an exemption to the restoration obligation; and**
  - **require the AFP to exercise separate powers of investigation, arrest and charge in relation to any offences that may be committed as a**

result of the person holding or operating the account (or separately make an application for a confiscation or restraining order under applicable proceeds of crime legislation).

Recommendation 51—Ombudsman oversight of account takeover warrants

- **The oversight functions of the Ombudsman in relation to account takeover warrants should be enhanced to incorporate the matters listed at paragraph [544] of this submission.**

Overarching matters concerning data disruption, network activity and account takeover warrants (Schedules 1-3) (recs 52-55 of 57)

Recommendation 52—specific protections: privileged & journalistic information

- **The issuing criteria and process for all three new warrant types should be subject to the protections listed in paragraph [548] of this submission, in relation to information subject to client legal privilege, and confidential journalistic information (including source identities).**

Recommendation 53—safeguards against exposure to multiple assistance orders

- **The Bill should be amended to insert further statutory pre-conditions to the issuance of all types of mandatory assistance orders under the SDA (existing and proposed), TIA Act, Crimes Act and Part 15 of the Telecommunications Act to require the issuing authority to consider:**
  - **the number of previous orders sought or issued in relation to the subject of a proposed order (by any agency); and**
  - **the likely cumulative impact on the person of being subject to multiple orders, and any third parties whose interests may be affected. (This may include, for example, the employer of a person, whose employee may be unavailable from their usual duties in order to comply with an order)**

Recommendation 54—availability of statutory judicial review rights for all warrant types (including consistent treatment of intelligence warrants)

- **The forthcoming corrections to the Explanatory Memorandum should specifically explain the effect of section 9A of the ADJR Act in relation to the three new warrant types proposed in the Bill.**
- **As the Bill proposes to make a type of intelligence-collection warrant (namely, network activity warrants) subject to statutory judicial review in accordance with section 9A of the ADJR Act, consideration should be given to extending this arrangement to cover some or all other types of intelligence collection warrants, such as ASIO's computer access warrants.**

Recommendation 55—sunset clauses and statutory review functions

- **The Bill should be amended to provide that:**

- **all of the new warrant-based powers are subject to a sunset clause of three years (or a period no more than five years); and**
- **the Committee is required to conduct a review of these warrant-based powers prior to their sunset date, to inform Parliamentary decision-making about whether they should be renewed.**

- **Consideration should be given to expanding the remit and resourcing of the INSLM to cover the operation of the new warrant-based powers in full, including the ability of the Committee to request the INSLM to undertake a review of these provisions, which could inform the subsequent Parliamentary pre-sunsetting review.**
- **Further consideration is needed for independent and Parliamentary oversight arrangements for criminal investigation powers and offences that have national security implications but are not directed exclusively to national security matters. If there is a desire for such functions to be performed by the Committee and the INSLM, then consideration should be given to the necessary legislative amendments and resource increases.**
- **The Australian Government *Legislation Handbook* should be amended to require all proposed national security legislation that seeks to confer new or significantly expanded powers to be subject to the following requirements (particularly in the case of novel or otherwise extraordinary powers, which are coercive or intrusive in nature):**
  - **routine consideration of whether the proposed measures should be subject to a sunset clause, and explicit documentation of the reasons for the ultimate policy decision in the Explanatory Memorandum to the Bill; and**
  - **the routine inclusion of statutory provisions requiring the conduct of independent and Parliamentary reviews after a period of operation, in the range of three to five years.**

Controlled operations (Schedule 4) (recs 56-57 of 57)

Recommendation 56—omission of Schedule 4 from the Bill

- **Schedule 4 should be omitted from the Bill, in recognition that the issues that have given rise to the perceived need for the amendments are, in fact, capable of being managed under the existing provisions governing the authorisation of controlled operations.**

Recommendation 57—amendment to section 15HC of the Crimes Act

- **To avoid any doubt or uncertainty, section 15HC of the Crimes Act should be amended to provide expressly that a controlled operation cannot authorise, or confer criminal immunity or civil indemnity for, activities in respect of which a data disruption warrant, or a network activity warrant is required under the SDA (or an emergency authorisation for these activities).**

Data disruption warrants (Schedule 1)

12. Schedule 1 to the Bill proposes to amend the SDA to enact the regime of data disruption warrants in new Division 5 of Part 2 of that Act. A data disruption warrant would authorise the AFP or ACIC to undertake activities to disrupt data held in a computer that is being used in the suspected commission of an offence ('**target computer'**) so as to frustrate the commission of that offence, or similar offences.

13. In addition to the threshold question of whether such powers should be conferred, contrary to the recommendation of the Richardson Review, the Law Council has identified several issues in the design and drafting of the provisions governing the proposed regime. These issues make it difficult to conclude that the proposed legislative framework for data disruption activities is proportionate to the objective of disrupting serious and harmful cyber-enabled crimes, where such intervention is independently confirmed to be reasonable and necessary in the circumstances.

14. If the Committee decides to support the proposed rejection of the Richardson Review recommendation that law enforcement agencies should not be conferred with specific disruption powers, then the Law Council's recommended amendments to provisions of Schedule 1 to the Bill would remove the most problematic areas of overbreadth in the proposed powers.

15. The Law Council's recommendations would also go some way towards protecting members of the community against the risk of serious loss or damage from any misuse or aberrant use of the proposed disruption powers. Even unintentional, good faith errors could have serious, adverse impacts on large numbers of lawful computer users, who are not suspected of any wrongdoing.

Threshold issue: should data disruption powers be conferred?

Richardson Review recommendations and reasoning

16. In its final report, provided to the Government in December 2019 and released publicly (in unclassified form) in December 2020, the Richardson Review concluded that law enforcement agencies, particularly the AFP, **did not** require new disruptive powers to combat cyber-enabled crime.[2]

17. Rather, the Richardson Review recommended that the AFP should obtain assistance from the Australian Signals Directorate (**ASD**) to improve its technical capabilities, which could be deployed in the exercise of the AFP's existing investigatory powers.[3] In reaching this conclusion, the Richardson Review placed weight on the following factors:

    - the AFP already has extensive disruption powers, including enforcing preparatory offences, conducting controlled operations, and exercising powers of seizure and forfeiture under proceeds of crime laws;[4]
    - the concept of 'disruption' in the context of cyber-enabled crime is 'nebulous' and capable of covering very wide spectrum of activities. For example, such activities may range from interference with communications to and from a particular child abuse website by launching a denial of service attack, through

[2] Richardson Review, *Unclassified Report,* Volume 3, (December 2019), 218-221 at [38.58]-[38.76] and recommendation 162.

[3] Ibid, recommendation 162.

[4] Ibid, 219 at [38.64].

to the destruction of physical property such as a computer, server or other ICT infrastructure;[5] and

- there are both practical and principled problems with the AFP, or any other law enforcement agency, being conferred with powers to destroy property.

18. On the latter point, the **practical problems** identified by the Richardson Review are:

- the risk of mistakes in targeting or execution (or both), which may have disastrous and far-reaching consequences for third parties who are using, or are otherwise reliant on, services provided via a computer system or network, and are not under any suspicion of criminal wrongdoing;[6] and
- in preparing to carry out a data disruption activity, the AFP is likely to obtain sufficient evidence to exercise its powers of arrest or seizure, which makes it impossible to conclude that a specific data disruption power is necessary.[7]

19. The Richardson Review also identified a number of **principled problems** in relation to a specific data disruption power for law enforcement agencies, primarily:

- conferring a specific data disruption power on the AFP 'risks compromising essential democratic rights' as it would empower police to make 'conclusive assessments of criminality'. This '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 power would be 'the equivalent of making the police the judge, jury and executioner, and this would raise fundamental consequences for the rule of law in Australia';[8] and
- it is not the lack of a specific statutory framework authorising the exercise of powers which are given the specific label of 'disruption' that 'holds the AFP back from being effective in disrupting online crime'. Rather, before it can be concluded that new statutory powers are necessary, there is first a need for the AFP to access and utilise stronger specialist skills, equipment and training to conduct effective disruption operations under its existing legislative powers. The Richardson Review considered that this option should be exhausted before specific disruption powers could be seriously contemplated.[9]

Alternative recommendation—judicial approval of disruption powers

20. The Richardson Review further recommended that, if its primary recommendation was not accepted and specific disruption powers were to be conferred on law enforcement agencies, then 'any disruption activity involving damage to or destruction of property should require judicial approval'.[10]

21. This alternative recommendation is significant in the context of other conclusions of the Richardson Review, which did not support a general requirement for all intelligence collection warrants to be subject to judicial authorisation.[11]

22. The Law Council disagrees, in the strongest possible terms, with the general recommendation and reasoning of the Richardson Review against the judicial authorisation of warrants. However, the fact that the Richardson Review made an

[5] Ibid, 220 at [38.66].
[6] Ibid, 220 at [38.68].
[7] Ibid, 220 at [36.69].
[8] Ibid, 220 at [38.70] and 221 at [38.73].
[9] Ibid, 221 at [38.74].
[10] Ibid, 221 at [38.76].
[11] Richardson Review, *Unclassified Report,* Volume 2, (December 2019), 60 at [18.111]-[18.1113] and recommendation 30.

exception for the authorisation of data disruption powers for cyber-enabled crime clearly conveys that such powers are of an even more extraordinary and entirely different character to warrant-based surveillance powers, which are exercised for the purpose of collecting intelligence or admissible evidence in relation to the target. The Richardson Review considered that the extraordinary nature of disruption powers should be reflected in the applicable authorisation requirements.

Government rejection of Richardson Review recommendation

Rejection of primary recommendation

23. The Government response to the Richardson Review, released in December 2020, disagreed with the recommendation against the conferral of specific disruptive powers. This reflected the Government's view that the current powers of the AFP and ACIC 'are increasingly ineffective against mass campaigns of cyber-enabled crime, including those that use the cover of the dark web and anonymising technologies on the surface web (such as virtual private networks)'.[12]

24. The Government response stated that new data disruption powers would be 'targeted at activities that have a direct and real impact on Australia's most vulnerable' (such as the online exploitation and sexual abuse of children) and activities 'orchestrated by the most sophisticated of criminal networks' (including the sale of illicit drugs and firearms, and terrorism-related activities).[13]

Rejection of alternative recommendation

25. The proposed data disruption warrant regime in Schedule 1 to the Bill further contradicts the alternative recommendation of the Richardson Review that, if specific disruption powers are to be conferred, they must be judicially authorised where property damage is involved.

26. As discussed below, the warrant-based data disruption powers proposed in the Bill will authorise physical property damage, as well as loss of or damage to data, if this is 'justified and proportionate'.[14] However, the Bill proposes to enable the Attorney-General to appoint as issuing authorities ordinary members of the Administrative Appeals Tribunal (**AAT**) who are admitted lawyers of just five years' standing (and need not have engaged in any legal practice following their admission).[15]

Law Council views: Richardson Review recommendation & Government response

27. The Law Council considers that the reasons advanced by the Richardson Review are persuasive and should be accepted, unless highly compelling evidence is presented publicly about significant changes to the security outlook since that review delivered its report in December 2019, which necessitates revision of its conclusions. No such evidence is presented in the Explanatory Memorandum to the Bill or the Government response to the Richardson Review.

28. Further, the Government response to the Richardson Review does not engage with the reasoning underlying the recommendation against the conferral of discrete data disruption powers. There is no evidence-based explanation of how the existing powers available to the AFP and ACIC are considered to be ineffective, including the

[12] Attorney-General's Department, *Commonwealth Government Response to the Comprehensive Review of the Legal Framework of the National Intelligence Community*, (December 2020), 12.

[13] Ibid.

[14] Bill, Schedule 1, item 15 (inserting proposed paragraphs 27KE(7)(b) and 27KE(12)(a) of the SDA).

[15] Ibid (inserting proposed subsection 27KA(2) and section 27KC of the SDA, which applies the defined term 'nominated AAT member' per existing section 13 of the SDA).

numerous, significant recent expansions of electronic surveillance powers (especially those conferred by the TOLA Act amendments in 2018).

29. There is also no engagement with the significant risks in relation to the matters of principle identified by the Richardson Review, as summarised at paragraph [19] above, which arise from the doctrine of the rule of law and the separation of powers.

30. If there is an appetite to proceed with the proposed data disruption powers in Schedule 1 to the Bill, then it is essential that the alternative recommendation of the Richardson Review is implemented. This would limit the classes of persons able to issue data disruption powers to judicial officers, who are appointed in a personal capacity. (The provisions of Schedule 1 to the Bill governing the eligibility and appointment of issuing authorities is discussed in detail from paragraph [89] below.)

Recommendation 1—implementation of Richardson Review recommendations

Preferred option

- **Schedule 1 should be omitted from the Bill, and recommendation 162 of the Richardson Review should be implemented in full.**

Alternative (non-preferred option)

- **If there is no appetite to implement recommendation 162 of the Richardson Review, Schedule 1 to the Bill should be amended consistently with the Law Council's recommendation 5 below. This would implement the alternative recommendation of the Richardson Review that data disruption powers should be authorised only by judicial officers, and not members of the AAT.**

Overview of proposed regime

31. The proposed data disruption regime would have the following attributes:

Issuing authority

- Data disruption warrants are issued by one of the following persons, if appointed by the Attorney-General as an issuing authority (which is consistent with the appointment of issuing authorities for other SDA warrants):
  - a judge of a court created by Parliament (for example, a State or Territory Magistrates' Court, or the Federal Circuit Court of Australia, Federal Court of Australia or Family Court of Australia); or
  - a member of the AAT who is either the President or a Deputy President, or an ordinary member who is an Australian-admitted lawyer of at least five years' standing (without any requirement to have engaged in legal practice, in relevant fields, for a set period after their admission).[16]

Applicant

- Any law enforcement officer of the AFP or ACIC, or any other person acting on behalf of those officers, may apply for a data disruption warrant.[17]

[16] Bill, Schedule 1, item 13 (inserting new section 27KC of the SDA). See also: SDA, sections 12 and 13 (definitions of 'eligible judge' and 'nominated AAT member' which are also used for data disruption warrants).

[17] Ibid (inserting new section 27KA of the SDA).

Issuing grounds

- Data disruption warrants may be issued if the issuing authority is satisfied that there are reasonable grounds on which to suspect that:
  - one or more 'relevant offences of a particular kind' (being offences punishable by a maximum penalty of three or more years' imprisonment) have been committed, or are being committed, or are about to be committed, or are likely to be committed;
  - those offences involve, or are likely to involve, data held in the target computer ('relevant data'); and
  - the issuance of the warrant is justifiable and proportionate, having regard to matters including:
    - the nature and gravity of the relevant offences;
    - the likelihood that data disruption will frustrate the commission of those offences; and
    - the existence of alternative means of frustration.[18]

Authorised activities

- Data disruption warrants **may authorise** a number of activities at the discretion of the issuing authority considering the application, including:
  - disrupting the relevant data, if this is likely to assist in frustrating the commission of the relevant offence(s) covered by the warrant. (The concepts of 'disruption' and 'frustration' are not defined in the Bill);
  - equivalent acts to those which are able to be authorised by computer access warrants under Division 4 of Part 2 of the SDA, namely:
    - entering premises;
    - using computers and other facilities and equipment for the purpose of accessing relevant data;
    - adding, altering and deleting data in a target computer or other computer;
    - temporarily removing computers and other things from premises;
    - conducting telecommunications interceptions for the purpose of doing any things specified under warrants;
    - materially interfering with a communication in transit to or from a computer, and the lawful use by third parties of a computer, if necessary to do one of the things specified in the warrant; and
    - concealing authorised actions taken under warrants, including after the warrant ceases to be in effect;[19] and
  - an act that is presently prohibited under the computer access warrant provisions in Division 4 of Part 2 of the SDA—namely, the causation of material loss or damage to other persons who are lawfully using a computer, provided that it is 'justified and proportionate, having regard to the offences covered by the warrant'.[20]

[18] Ibid (inserting new sections 27KA and 27KC of the SDA).
[19] Ibid (inserting new subsections 27KE(2)-(7) and (9) of the SDA).
[20] Ibid (inserting new subsection 27KE(10)(b) of the SDA).

- All data disruption warrants **must authorise** a number of activities, namely:
  - the use of force against persons and things, if reasonable and necessary to do the things specified in the warrant; and
  - if the warrant authorises entry to premises, the warrant must specify the hours of entry, or state that entry is permitted at any time.[21]

Extraterritoriality (offshore data access and disruption activities)

- Data disruption warrants may apply extraterritorially, if an authorised official of the foreign country has consented to the doing of an act in that country.[22]

Duration of warrants

- Data disruption warrants are in force for up to 90 days,[23] and are able to be extended for up to 90 days (giving a total maximum duration of 180 days).[24]

Persons who may exercise authority under a warrant

- The Bill does not provide that only law enforcement officers who are members of the AFP or ACIC (as applicable) may exercise authority under a data disruption warrant. Nor does it provide a statutory framework for the authorisation of other persons to execute warrants for, and on behalf of, the AFP or ACIC.[25]
- However, the Law Council understands from remarks of the Minister for Home Affairs in August 2020, prior to the introduction of the Bill, that there is an intention, at least in some cases, for the disruption component of these warrants to be undertaken by staff of ASD who will be made available to the AFP and ACIC.[26]

Authorised applicants

Scope of proposed power

32. Proposed subsection 27KA(1) of the SDA provides that any 'law enforcement officer' of the AFP or ACIC may make an application for a data disruption warrant. The term 'law enforcement officer' is defined in existing section subsection 6A(3) of the SDA and relevantly covers all employees of, and secondees to, the AFP and ACIC.

33. In addition, proposed subsection 27KA(1) purports to authorise 'another person' to make the application on behalf of such a law enforcement officer. Such persons are not limited to any other law enforcement officer of the relevant agency. Nor is there

[21] Ibid (inserting new subsection 27KE(8) of the SDA).

[22] Ibid, Schedule 1, item 27 (inserting new section 43C of the SDA).

[23] Ibid, Schedule 1, item 13 (inserting new subsection 27KD(2) of the SDA).

[24] Ibid (inserting new subsections 27KF(1) and (6) of the SDA).

[25] Ibid, (inserting new subsection 27KE(1) of the SDA, which is drafted in the passive voice: 'a data disruption warrant must authorise the doing of specified things' without identifying who is authorised to do those things). While proposed subparagraph 27KD(1)(b)(viii) requires the warrant to specify the 'name of the law enforcement officer primarily responsible for executing the warrant' there is no requirement to specify who is authorised to do the individual acts specified in the warrant, under the primary responsibility of that law enforcement officer. In contrast, intelligence legislation prescribes specific processes for the authorisation of persons to exercise authority under a warrant. See, for example, *Australian Security Intelligence Organisation Act 1979* (Cth), section 24; and *Telecommunications (Interception and Access) Act 1979* (Cth), section 12.

[26] The Hon Peter Dutton MP, Minister for Home Affairs, *Transcript of joint press conference with the Prime Minister*, Parliament House, Canberra, 6 August 2020.

any requirement for the 'other person' to be a staff member of the AFP or ACIC, who has been authorised by the agency head to make such applications (whether as part of a class of persons by reference to their position or rank, or individually).

The need for stronger statutory parameters

34. The Law Council considers that stronger statutory parameters are needed with respect to the persons who may make applications for these warrants. This is necessary in view of the novel nature of data disruption powers, the potentially significant consequences for non-suspects,[27] together with the broad thresholds and intricate nature of the statutory issuing test.

35. While it may be the case that the AFP and ACIC may, from time-to-time, adopt internal policies and other administrative governance requirements that limit the classes of persons able to apply for data disruption warrants, the Law Council considers that these matters should be dealt with directly in primary legislation, rather than being reliant solely upon executive discretion in the exercise of powers.

36. A more judicious and focused statutory authorisation of applicants, which is limited to AFP and ACIC members of who possess a prescribed level of seniority and expertise, will offer greater assurance in relation to the rigour and consistency of quality of applications for data disruption warrants.

37. Such assurance is particularly important for members of the public, who will generally not see warrant applications or internal policies governing who may make applications for authorisations to exercise extraordinary data disruption powers. Applying stronger statutory parameters to the authorisation of persons to apply for warrants is also likely to assist issuing authorities, who may be required to determine complex applications in compressed timeframes.

38. The Law Council emphasises that it is no answer to simply identify that the Bill appropriates the existing provisions of the SDA, which specify the persons who may apply for other types of warrants under that Act (for example, warrants authorising the use of surveillance devices and computer access for investigative purposes).[28]

39. Such an approach would incorrectly assume that the existing 'baseline' governing other warrant applications in the SDA is appropriate for any intrusive power. Moreover, the proposed data disruption powers are novel and could have highly significant, adverse impacts on the rights and liberties of non-suspects, which far exceed the adverse impacts that may arise from actions taken under computer access or surveillance device warrants. Those adverse impacts may arise from activities within the scope of the authority of the warrant. However, as the Richardson Review cautioned, they may also result from acts that exceed the scope of lawful authority conferred under the warrant, through error or inadvertence.[29]

Recommendation 2—persons who may apply for data disruption warrants

- **Proposed subsection 27KA(1) of the SDA (item 13 of Schedule 1) should be amended so that the persons who are authorised to apply for a data disruption warrant are those who meet the following requirements:**

[27] For example, lawful computer users who are reliant on websites or other online services (including essential services that are delivered online) which are disrupted as a result of a data disruption warrant, and may suffer loss or damage as a result of interruption.

[28] SDA, subsections 14(1) (surveillance device warrants) and 27A(1) (computer access warrants).

[29] Richardson Review, *Unclassified Report,* Volume 3, (December 2019), 229 at [36.68].

- **the person is a law enforcement officer in relation to the AFP or ACIC (as applicable) within the meaning of section 6A of the SDA; and**
- **the person holds a position within the AFP or ACIC (as applicable) that is of a minimum, prescribed level of seniority, which should not be any less than an Executive Level 2 under the *Public Service Act 1999* (Cth) or an equivalent rank; and**
- **the person has been approved, by written instrument made by the AFP Commissioner or ACIC CEO (as applicable) to apply for data disruption warrants (either by class or individually); and**
- **the relevant agency head must not approve a person under the above requirement, unless satisfied on reasonable grounds that:**
  - **the person holds a supervisory role in the chain of command;**
  - **it is necessary and proportionate for the person to apply for data disruption warrants in the course of their normal duties with the AFP or ACIC (as applicable); and**
  - **the person possesses the requisite skills, knowledge and experience to make warrant applications, and the person has completed all current internal training requirements for making such applications.**

Issuing criteria

'Relevant offences' subject to disruption warrants

40. The public policy justification advanced in support of the proposed data disruption power focuses on targeting and frustrating offences of the most serious and harmful nature. It focuses primarily on those offences from which there is a strong need to protect vulnerable members of the community from serious harm, such as child exploitation and terrorism.[30]

41. However, the Bill does not give precise expression to this intent. The proposed issuing thresholds for data disruption warrants far exceed the types of offences described in the Explanatory Memorandum. The Bill proposes to permit warrants to be obtained in relation to the suspected commission of a 'relevant offence'. This term is defined in existing section 6 of the SDA as covering, among other matters:

> *(a) an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life; or*
>
> *(b) an offence against a law of a State that has a federal aspect and that is punishable by a maximum term of imprisonment of 3 years or more, or for life; or*
>
> ***
>
> *(e) an offence that is prescribed by the regulations.*

[30] See, for example: Explanatory Memorandum,26 at [45] ; and Attorney-General's Department, *Commonwealth Government Response to the Comprehensive Review of the Legal Framework of the National Intelligence Community*, (December 2020), 12.

Offences punishable by a maximum penalty of 3 or more years' imprisonment

42. The Explanatory Memorandum states that the linkage of warrant-based data disruption powers to 'relevant offences' will 'limit the availability of data disruption warrants only to the most serious offence categories, such as terrorism and child exploitation'.[31]

43. In fact, innumerable Commonwealth offences and State offences with federal aspects are punishable by a maximum penalty of three or more years' imprisonment, which have no rational connection with such offending. Many such offences cover criminality at the lower end of objective seriousness.

Examples of Commonwealth offences that would be eligible for disruption warrants

44. By way of illustration, paragraphs (a) and (b) of the definition of a 'relevant offence' in existing section 6 of the SDA would enable data disruption warrants to be sought and issued in relation to the following kinds of offences, where they are suspected of being carried out using data held in a computer:

- **copyright infringement:** offences for the infringement of copyright under Part V the *Copyright Act 1968* (Cth) (which may also involve subjective judgments about the existence of criminal fault elements in relation to certain circumstances, which will determine whether the particular offence meets the penalty threshold for the issuance of a disruption warrant);

- **theft, deception and dishonesty offences** against the Commonwealth under Chapter 7 of the *Criminal Code Act 1995* (Cth) (**Criminal Code**);

- **secrecy offences:** official secrecy offences under Part 5.6 of the Criminal Code for unauthorised disclosures of, or dealings with, certain official information. These offences apply to current and former Commonwealth officials, as well as other persons who may access official information, including journalists who receive it from their sources. The task of executing data disruption warrants issued in connection with such offences is likely to be particularly complicated because of the extensive defences to those offences in section 122.5 of the Criminal Code (including the defence in subsection 122.5(6) for journalists reporting on public interest matters). If a person legitimately relied upon a defence to a secrecy offence, there is a risk that the relevant exculpatory circumstances may not necessarily be evident to the law enforcement officers who obtained and executed the data disruption warrant. It is therefore possible that the covert act of data disruption may be authorised and completed, and the damage sustained, before the existence of the exception becomes apparent to the relevant AFP or ACIC officers;

- **offences relating to the use of telecommunications carriage services** in Division 474 of the Criminal Code, including:

  - the offence in **section 474.17** for using a carriage service, such as the internet, to menace, harass or cause offence (which covers a wide spectrum of conduct);[32] and

[31] Explanatory Memorandum, 26 at [45].

[32] See, for example, *Monis v The Queen; Droudis v The Queen* (2013) 249 CLR 92 at [29] and [55]-[59] (per French CJ). The High Court endorsed the interpretation of the NSW Court of Criminal Appeal that the concept of 'cause offence' in section 474.17 of the Criminal Code did not extend to mere 'hurt feelings' but did

- the offence in **section 474.47** for using a carriage service, such as the internet, to incite property damage or theft on agricultural land. This could include use of the internet by animal rights groups to organise protests, or covert evidence gathering activities at abattoirs or farms.

  The application of the data disruption warrant regime to such offences could be particularly challenging in light of the specific exceptions in subsection 474.47(2) for a person who disseminates materials in their capacity as a professional journalist, for the purpose of making a news report of matters in the public interest. It would mean that the law enforcement officers seeking to obtain and execute a data disruption warrant in these circumstances would need to consider whether the person is a 'professional journalist', and whether the matter was in the public interest. If the judgments of those officers are later found to be incorrect, it will be too late to prevent the damage caused by the acts of data disruption purportedly carried out under the warrant.

  Similarly, law enforcement officers seeking or executing a disruption warrant in relation to an offence against section 474.47 of the Criminal Code would need to make a unilateral assessment of whether the severance provision in section 474.48 applied, to exclude the application of the offence where it would contravene the implied constitutional freedom of political communication. This will likewise require law enforcement officers to make extremely complex and intricate judgments on matters of constitutional law, in the context of decision-making about whether to seek or execute a disruption warrant.

  This heightens the warning sounded by the Richardson Review that a data disruption power has the potential to effectively make law enforcement officials the 'judge, jury and executioner'. Even where data disruption powers have been independently authorised under warrant, there is still considerable scope for value judgment about whether particular actions are within the scope of that authorisation, at the point of executing the warrant and undertaking data disruption activities;[33]

- **breaches of public health directions:** breaches of directions or orders made under the *Biosecurity Act 2015* (Cth) (**Biosecurity Act**) while a declaration of a biosecurity emergency is in force. This could include, for example, people who use a computer to organise protests or other activities on social media or online chat groups, which may breach Commonwealth directions made under the Biosecurity Act, in respect of the current *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) Declaration 2020*;

- **corporate criminal offences:** breaches of certain directors' duties under the *Corporations Act 2001* (Cth) (for example, duties to act in good faith and in the best interests of the company; and duties not to use their position or information obtained from their position dishonestly, with the intention of gaining personal advantage or causing detriment to the company);[34]

- **breaches of control order conditions:** offences against section 104.27 of the Criminal Code by persons who are subject to control orders, and breach

cover any conduct that was 'calculated or likely to arouse significant anger, significant resentment, outrage, disgust, or hatred in the mind of a reasonable person in all the circumstances'.

[33] Richardson Review, *Unclassified Report*, Volume 3, (December 2019), 221 at [38.73].

[34] *Corporations Act 2001* (Cth), sections 184, 1311E and Schedule 3. These offences are punishable by a maximum penalty of 15 years' imprisonment.

applicable conditions of that order prohibiting or restricting their use of a computer or the internet. The data disruption powers would be available even if the person used a computer or the internet for benign purposes that did not pose any national security threat. (Equivalent issues will arise in relation to conditions of extended supervision orders, if the Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Bill 2020 presently under inquiry by the Committee is passed); and

- **State and Territory offences:** an indeterminate range of State offences that are deemed to have a federal aspect, by reason of section 7 of the SDA, which imports definitions from section 4AA of the *Australian Federal Police Act 1979* (Cth) (**AFP Act**) and section 4A of the *Australian Crime Commission Act 2002* (Cth) (**ACC Act**). In effect, this is any State offence as in force from time-to-time that the Commonwealth Parliament would have had legislative power to enact itself (provided the maximum penalty is at least three years' imprisonment). This will cover a highly extensive range of fields, potentially including offences under State or Territory emergency management legislation governing responses to public health emergencies, such as the present COVID-19 pandemic.

Future expansions of offences covered by paragraphs (a) and (b)

45. It should be noted that the range of offences covered by paragraphs (a) and (b) of the definition of a 'relevant offence' in section 6 of the SDA is not static until such time as the Parliament passes legislation to expressly amend it.

46. Rather, the definition of a 'relevant offence' will expand automatically whenever the Australian Parliament enacts a new offence that meets the three-year penalty threshold, or increases the maximum penalty for an existing offence which would bring it within the penalty threshold for data disruption warrants.

47. There is no mechanism in the Bill to ensure that Parliament is specifically alerted to the fact that proposals for new offences, or increases to penalties for existing offences, will expand the range of offences covered by paragraphs (a) and (b) for the purpose of the proposed data disruption warrant regime. Consequently, there is no explicit Parliamentary approval mechanism for such expansions.

48. The Law Council submits that, as a matter of practicality, it is unlikely that all members of the Australian Parliament would proactively have the data disruption warrant regime in their specific contemplation, when scrutinising legislation containing proposed offences of general application, which have no clear subject matter-based connection with the most serious and harmful kinds of offences that the data disruption regime is intended to target.

49. Similarly, whenever a State Parliament enacts a law containing an offence punishable by a maximum penalty of three or more years' imprisonment, that offence will likely enliven the Commonwealth data disruption regime, if the subject matter of the offence falls within the concurrent legislative power of the Commonwealth. Given that the enumerated heads of legislative power in section 51 of the Commonwealth Constitution cover a wide range of fields, there is likely to be an extensive range of current and future State offences that will enliven paragraph (b) of the definition of a 'relevant offence' and will therefore be eligible for data disruption warrants.

50. The members of all State Parliaments may not necessarily routinely consider the potential enlivenment of the Commonwealth data disruption warrant regime, when enacting or amending general offences under their own jurisdiction's legislation.

This is especially because it is likely that the subject matter of such offences will not have any self-evident connection with the data disruption powers of federal law enforcement bodies.

Offences prescribed by regulation

51. Paragraph (e) of the definition of a 'relevant offence' in existing section 6 of the SDA covers any offence that is prescribed by the regulations, irrespective of its maximum penalty. The Law Council is concerned that this will result in an inappropriate delegation of legislative power to the executive government to determine the offences that will enliven the proposed data disruption regime.

52. A novel and extraordinary power such as data disruption requires a high degree of Parliamentary supervision and control. The Law Council considers that limiting the functions and powers of the Parliament merely to disallowing regulations, after they have been made and have commenced, is not proportionate to the gravity of data disruption powers. Specific concerns are set out below.

Risk of low-level offences being subject to data disruption warrants

53. At the time of writing this submission, no regulations were in force for the purpose of paragraph (e) of the definition of 'relevant offence' in section 6 of the SDA.

54. Nonetheless, the proposal for data disruption warrants to be available in connection with 'relevant offences' within the meaning of existing section 6 means that it would be legally possible for regulations to be made which prescribe offences punishable by a lesser maximum penalty than the threshold of three years' imprisonment for the purpose of paragraphs (a) and (b) of the definition of 'relevant offence'. In this event, it would be legally possible for data disruption warrants to be issued in relation to a wide range of minor offences.

Risk of automatic, unintentional enlivenment of data disruption warrant regime

55. If regulations are made under paragraph (e) to prescribe a particular offence or offences as 'relevant offences' for the purpose of the SDA, this would automatically enliven all of the warrant-based powers in relation that offence or those offences.

56. The Law Council is concerned that the proposal to tie data disruption warrants to the existing definition of a 'relevant offence', including paragraph (e), means that there is no statutory requirement for the Governor-General-in-Council (and those advising them) to specifically consider, and be satisfied of, the necessity and proportionality, of enlivening data disruption powers in respect of each offence prescribed in regulations. Any such consideration would be at the sole discretion of the Executive Government in individual cases. Reliance on unguided executive discretion is not a safeguard which imposes a legal requirement for a power to be exercised in a proportionate way, which takes account of all relevant considerations.

Disallowance alone is an insufficient form of Parliamentary oversight

57. While the Parliament would have the power to disallow regulations made under paragraph (e) of the definition of 'relevant offence', the Law Council considers that disallowance is not a proportionate form of Parliamentary control over the proposed data disruption powers.

58. A data disruption power is of a fundamentally different nature to a power of surveillance, and this difference should be reflected in the nature of Parliamentary oversight in relation to the data disruption warrant regime. Data disruption is

directed to frustrating the commission of an offence and involves active intervention in criminal conduct. In contrast, surveillance is generally directed to the purpose of investigating and collecting admissible evidence in relation to a suspected offence, for the ultimate purpose of prosecuting a person. Surveillance carried for investigative and enforcement purposes necessarily cannot involve active intervention in the suspected criminal conduct, other than via the arrest of the person on suspicion of an offence or offences (or potentially also through the exercise of powers of seizure under a search warrant, or making a confiscation application under proceeds of crime legislation).

59. For this reason, the power to extend the coverage of 'relevant offences' by regulation should not apply automatically to warrant-based powers of disruption. Rather, there should be a requirement for the Parliament to specifically approve the proposed extension of the data disruption warrant regime any further offences. In contrast, Parliamentary disallowance of a legislative instrument is a discretionary political remedy, which is contingent on a range of external circumstances, including party political considerations and competing items of Parliamentary business. Such discretion is no substitute for a legally binding safeguard.

60. Moreover, the power of disallowance is exercisable **after** the relevant regulations have been made, and generally after they have commenced (noting that commencement normally occurs the day after registration).[35] This means that, if the Parliament considers that the regulations have prescribed an offence or offences that inappropriately extend the scope of the data disruption regime, then the expanded data disruption regime will have been operational for a period of time before the Parliament has an opportunity to disallow those regulations. This could be protracted where the Parliament has adjourned for an extended period, such as scheduled sitting breaks, or unscheduled adjournments (as occurred due to the COVID-19 pandemic in 2020).

61. Accordingly, the Law Council recommends that, if the disruption warrant regime is to be enacted, the categories of offences covered by those warrants should be prescribed **exhaustively** in primary legislation. This is necessary to ensure that the Parliament exercises a degree of control over the regime, which is commensurate with the extraordinary nature of data disruption powers.

Aspects of the issuing test which aggravate the overbreadth in the concept of a 'relevant offence' for the purpose of the data disruption regime

62. In considering the scope of a 'relevant offence' as the basis for the disruption power, it should also be acknowledged that proposed subsection 27KA(1) of the SDA contains two further attributes that widen its scope and compound the overbreadth arising from paragraphs (a) and (b) of the definition of 'relevant offence'. Namely:

    - **low requirements of particularisation**—data disruption warrants are not required to individually particularise the suspected 'relevant offence' or 'relevant offences' in respect of which data disruption powers are authorised (including the ability to cause material loss or damage to third parties, where considered to be 'justified and proportionate'). Rather, it is sufficient for the law enforcement officer applying for the warrant to hold a reasonable suspicion that a relevant offence of a 'kind' (or category) has been committed, is being committed, or is likely to be committed. This means that, if a warrant is issued, the law enforcement officers executing that warrant will have to make complex and potentially subjective judgments about whether particular

[35] *Legislation Act 2003* (Cth), section 12.

online activity they identify while executing a warrant constitutes a 'relevant offence' that is covered by the 'kind' or category of relevant offences specified in the warrant. Those officers will need to make that assessment in the context of determining whether they are authorised to exercise highly intrusive powers of data disruption, with significant adverse consequences if that judgment is incorrect. The wider the definition of 'relevant offence', the more complex and uncertain that assessment will be, and the greater the risk of error; and

- **Prediction of future criminality**—data disruption warrants would authorise data disruption activities in relation to offences that are suspected of being 'about to' or 'likely to' be committed. This means that a prediction must be made about the future commission of a potentially very broad category of offences. The task of making predictions about future criminal conduct is fraught in any context, especially where that prediction is the basis for authorising a highly intrusive power that has the potential to cause significant loss, damage and disruption to a large number of people, including non-suspects.

63. The implications of these matters, in adding complexity and uncertainty and increasing the risk of error in executing warrants, are detailed further below.

64. The Law Council submits that these matters tend in further support of more tightly limiting the eligible offences for data disruption warrants to the most serious and harmful forms of offending described in the extrinsic materials to the Bill. This could avoid or significantly minimise risks of error in the exercise of data disruption powers, which may cause significant loss, damage or interference to non-suspects. (The Law Council has made a recommendation below for how the eligible offences could be limited further. It draws upon previous recommendations of the Committee in its inquiry into the impacts of investigative powers on media freedoms.)

Low requirements of particularisation

65. The concept of a 'kind' of offence will be open to interpretation by law enforcement officers at the point of deciding whether to exercise data disruption powers. (That is, they will need to decide whether a particular activity that they observe online is likely to constitute an offence which falls within the 'kind' of 'relevant offences' specified in the warrant instrument, and therefore covered by the warrant.) The Bill does not provide any coherent statutory decision-making principles for such assessments. The Law Council is concerned about the potential for ambiguity and overbreadth in the absence of clear guidance. For example:

- is the essential organising principle for determining a 'kind' of offence the **subject-matter of an offence?** On this assessment, a disruption warrant that specified child exploitation offences, or terrorism-related offences, could authorise data disruption in relation to all offences whose subject matter covered activities in the nature of child exploitation or terrorism. (It would not be limited to offences criminalising specific acts of child exploitation or terrorism, such as grooming children or financing a terrorist organisation); or
- could a 'kind' of offence cover multiple, disparate offences that are directed to a **common criminal purpose** by a single entity? On this assessment, the highly diversified criminal activities of an organised crime group (such as drug and firearm trafficking, and the laundering of proceeds of crime) would all be capable of being covered by a single data disruption warrant; and
- how would the concept of a 'kind' of offence operate in relation to suspected **money laundering offences and predicate offences?** In particular:

- Where a data disruption warrant is issued for 'relevant offences' comprising suspected money laundering offences, would the 'predicate offences' (being the underlying offences from which the money or property was derived, such as drug or firearms trafficking) amount to the same 'kind' of offence as the money laundering offences specified in the warrant as the 'relevant offences'?

- Conversely, if a data disruption warrant is issued for a suspected 'predicate offence' to a money laundering offence, could it also support disruption activities in relation to subsequent money laundering offences? If so, could this interpretation be supported even if the linkage between the suspected predicate offence(s) and money laundering offence(s) was unknown when the data disruption warrant was sought and issued?

66. It is clear that the question of whether an individual offence falls within the 'kind' of offence specified in a disruption warrant will require complex assessments of fact. The broader the range of offences eligible for data disruption warrants, the more complex these assessments will become.

67. Even if the meaning of a 'kind' of offence was limited to the subject-matter of a suspected offence, to the exclusion of offences in pursuit of a common criminal purpose, significant practical complexities and difficulties are still likely to arise.

68. For example, the key difference between the terrorism and foreign incursions offences in Parts 5.3 and 5.5 of the Criminal Code is that only terrorism offences require proof of an intention to cause serious harm in pursuit of a political, religious or ideological objective.[36] The foreign incursions offences in Part 5.5 apply to 'hostile activities' which involve the same acts or threats of harm as terrorism offences, but do not require proof of the additional element of political, religious or ideological motivation.[37] This fine distinction is likely to be relevant in assessing whether a disruption warrant issued in respect of a terrorism offence or offences against Part 5.3 of the Criminal Code is sufficient to authorise data disruption in relation to a suspected foreign incursions offence against Part 5.5.

69. The Law Council considers that this considerable scope for uncertainty, and consequent overbreadth and error, tends strongly in support of placing stronger statutory limits on the range of eligible offences for data disruption warrants, in line with the below recommendation. Those limits should be imposed directly in primary legislation and should not be capable of expansion by legislative instrument.

Prediction of future criminality

70. Data disruption warrants are able to be issued on the basis of a prediction of a person's future criminal conduct, not only a reasonable suspicion of the person's previous or current criminal conduct.

71. The task of predicting future criminality is extremely difficult and unreliable in any setting, especially where that prediction is the basis for exercising intrusive or coercive powers. Making such predictions in the context of issuing and executing data disruption warrants is likely to be even more fraught, because of the breadth of the definition of a 'relevant offence' and the ability for warrants to be issued on the basis of a prediction that a 'kind' or category of relevant offence is about to be, or likely to be, committed. This means that the law enforcement officers executing a

[36] Criminal Code, section 100.1 (definition of a 'terrorist act').

[37] Ibid, section 117.1 (paragraph (b) of the definition of 'engages in a hostile activity').

warrant will need to make complex decisions about whether exercising a power of data disruption would be likely to frustrate the future commission of a relevant offence, which is of the same 'kind' as those specified in the warrant instrument.

72. This task is likely to be especially complex where a suspected 'future offence' forms part of a scheme of 'tiered' offences under Commonwealth law, or a State law with a federal aspect. Such schemes typically involve multiple offences with a common or substantially similar set of physical elements, and a gradation of fault elements. The maximum penalties for each offence are also gradated, in line with the degree of culpability in the applicable fault element. (For example, the fault element of knowledge in relation to a circumstance will involve a higher degree of culpability than recklessness.)

73. Some offences in higher 'tiers' of the scheme may meet the three-year penalty threshold for data disruption warrants, but offences in the lower 'tiers' of the scheme may not. A significant example of a regime of 'tiered' offences is the money laundering offences in Division 400 of the Criminal Code. Some of the lower-value money laundering offences, and offences for dealing with proceeds of crime, carry a maximum penalty of less than three years' imprisonment.[38]

74. Consequently, it is conceivable that the process of determining applications for data disruption warrants to frustrate the suspected future commission of one or more offences under a tiered scheme could require very fine, and potentially subjective, judgments to be made about the existence of a particular criminal fault element. This exercise is likely to be especially difficult in the context of making a prediction about the future commission of an offence.

75. For example, an offence which applies a fault element of recklessness in relation to a circumstance might not meet the three-year penalty threshold for a disruption warrant. However, an offence at a higher 'tier' in the same statutory scheme that applies the fault element of knowledge to the same circumstance might meet the penalty threshold for a disruption warrant. The AFP or ACIC, as prospective warrant applicant, would have to assess which offence was 'likely' or 'about' to be committed.

76. The broader the range of offences that are made eligible for data disruption warrants, the more pronounced this problem will become. Conversely, if the eligible offences for data disruption warrants were more tightly limited to the most serious and harmful forms of offending referred to in the extrinsic materials to the Bill, this risk could be avoided or at least minimised significantly.

Recommended narrowing of eligible offences for data disruption warrants

77. The Law Council considers that the factors discussed above tend strongly in favour of narrowing the range of offences in respect of which data disruption warrants may be issued. These 'eligible offences' should be:

    - limited specifically to match the stated policy intent of targeting criminality of the most serious and harmful kind, from which there is an immediate need to

[38] See, for example, Criminal Code, subsections 400.6(3), 400.7(2), 400.7(3), 400.8(1)-(3) and 400.9(1A). Additionally, if data disruption warrants are sought in respect of suspected money laundering offences, there will also be a question of whether the partial defence of 'mistake of fact as to value of money or property' in section 400.10 applies. This would limit a person's culpability to a lower tier offence covering the lower value they mistakenly believed the money or property to be. This could reduce a person's liability to a lower tier of offence that falls short of the three-year maximum penalty threshold for a data disruption warrant. Law enforcement officers would have to assess whether section 400.10 was likely to apply at the time of deciding whether to exercise disruption powers under a data disruption warrant.

protect the community, or classes of vulnerable persons in the community, from predatory or exploitative behaviour; and

- prescribed exhaustively in primary legislation, so that the addition of further kinds of offences is subject to specific Parliamentary approval via the passage of legislation.

78. Given the novel and serious nature of disruption powers, the Law Council supports a targeted and judicious approach to determining the 'eligible offences'. This could be reviewed after the regime has been operational for a further period of time. The Law Council recommends that the following requirements should apply:

- the offence is indictable;
- the offence is punishable by a maximum penalty equivalent to the threshold for telecommunications interception warrants in paragraph 5D(2)(a) of the TIA Act (being seven years' imprisonment or more); and
- the offence covers the following subject-matter:
  - offences against the security of the Commonwealth in Chapter 5 of the Criminal Code;
  - offences against humanity and related offences in Chapter 8 of the Criminal Code (including child exploitation and human trafficking); and
  - consideration could also be given to including the following offences:
    - certain offences in Chapter 9 of the Criminal Code (covering dangers to the community) including serious drug, weapons and criminal association offences; and
    - certain money laundering and cybercrime offences in Chapter 10 of the Criminal Code.

Recommendation 3—'relevant offences' for data disruption warrants

- **Proposed section 27KA of the SDA (Schedule 1, item 13) and subsequent provisions in new Division 5 of Part 2 should be amended to make the following changes to the offences which are eligible for a data disruption warrant:**
  - **omit the concept of a 'relevant offence' within the meaning of section 6 of the SDA; and**
  - **replace it with the approach specified at paragraphs [77]-[78] of this submission.**

Assessment of necessity and proportionality: ss 27KC(1) and (2)

79. Proposed section 27KC prescribes the issuing criteria for data disruption warrants. Under proposed subsection 27KC(1), the issuing authority must be satisfied that:

- there are **reasonable grounds for the suspicion founding the warrant application**—that is:
  - a relevant offence has been committed, is being committed, is about to be committed or is likely to be committed—and, in all cases, the offence involves data held in a computer;
  - the likelihood that the disruption of data will substantially assist in frustrating the commission of a relevant offence of the same kind as the

offence which is mentioned in the point above. (In other words, this does not need to be the exact 'relevant offence' that is suspected); and

- proposed paragraph 27KC(1)(b) requires the issuing authority to be satisfied that 'the disruption of data authorised by the warrant is 'justifiable and proportionate' having regard to the relevant offences specified in the warrant application, which the AFP or ACIC seeks to frustrate.

80. In applying this test, the issuing authority must consider the non-exhaustive factors set out at subsection 27KC(2). These factors cover the nature and gravity of the relevant offences, the likelihood that data disruption will frustrate the commission of the relevant offence, and the existence of alternative means of doing so.

81. The Law Council welcomes the express issuing criterion of proportionality, and the mandatory considerations in applying that test. However, it recommends two amendments, which are directed to the following matters:

- an addition to the list of mandatory considerations in applying the proportionality test in proposed subsection 27KC(2); and
- substituting the issuing threshold of 'justifiable' in proposed paragraph 27KC(1)(b) with an issuing threshold of 'reasonably necessary'.

Further mandatory considerations in assessing proportionality: s 27KC(2)

82. The Law Council considers that there should be a specific statutory requirement for the issuing authority to be given information about the following matters, and to consider them in applying the issuing tests:

- the specific nature of the data disruption activities that are proposed to be carried out under the warrant;
- the nature and extent of the potential adverse impacts of those activities on non-suspects; and
- the steps proposed to be taken by the AFP or ACIC (as applicable) to avoid or minimise those impacts, and the anticipated effectiveness of those steps.

83. This reflects that any analysis of proportionality requires a comprehensive, evidence-based assessment of all the relative benefits and detriments that will, or are likely to, accrue to all persons who are likely to be affected by an action. The Law Council's recommended additions to the non-exhaustive matters specified in proposed subsection 27KC(2) will provide clear and consistent guidance to applicants and issuing authorities, thereby facilitating consistency in the identification and assessment of these matters across all warrant applications.

84. The consistent identification and assessment of reasonably foreseeable impacts on third parties is particularly important in view of an authorisation provision in proposed paragraph 27KE(7)(b) in relation to the acts which are permitted under disruption warrants. This would authorise, and therefore immunise, acts which are likely to cause material loss or damage to other persons lawfully using the computer, if such acts are considered to be justified and proportionate. Currently, computer access warrants issued under both the SDA and ASIO Act categorically prohibit the ACIC, AFP and ASIO from carrying out acts which are likely to cause such loss or damage.[39] The proposed data disruption regime is therefore novel in this respect. This should be reflected in the applicable issuing thresholds, including the degree of

[39] SDA, paragraph 27E(5)(b); and ASIO Act, paragraph 25A(5)(b).

statutory guidance provided in applying the issuing criteria of proportionality to the circumstances of individual warrant applications.

Threshold of 'reasonably necessary' rather than 'justified': s 27KC(1)(b)

85. Given the extraordinary nature of data disruption powers, including an ability to cause material loss or damage to third-party computer users who are acting lawfully, the Law Council considers that the issuing threshold for data disruption warrants should include a requirement that the issuing of the warrant is 'reasonably necessary' to frustrate the commission of the offence. A threshold of 'reasonable necessity' should replace the threshold in proposed paragraph 27KC(1)(b) that the issuing of the warrant is 'justified'

86. The Law Council acknowledges that a threshold of reasonable necessity could operate as a *de facto* 'last resort' condition. That is, an assessment of the necessity of proposed data disruption activities would require meaningful consideration, and exclusion, of potential alternative means of frustrating the commission of an offence. (Examples of alternatives may include exercising powers of arrest and charge, or commencing criminal confiscation proceedings under proceeds of crime legislation. These alternative powers could be exercised on the basis of evidence obtained under an investigative warrant, such as a computer access warrant issued under existing Division 4 of Part 2 of the SDA.)

87. However, if such a requirement should not be regarded as an unnecessary legal impediment to the proposed disruption powers, or an administrative burden on the responsible agencies. Rather, it would be a vital safeguard to a novel and extraordinary power, which far exceeds existing powers of surveillance for evidence collection purposes.

88. Further, it should be noted that the 'equipment interference' powers conferred on GCHQ (the UK signals intelligence and information assurance agency, equivalent to ASD) under the *Investigatory Powers Act 2016* (UK) (**IPA**) operate on a threshold of necessity, as well as an express statutory requirement of proportionality. These warrants are also subject to judicial approval under a 'double lock' issuing process.[40] Warrants, and actions taken under them, are also subject to review by the UK Investigatory Powers Tribunal under the *Human Rights Act 1998* (UK).[41]

Recommendation 4—stronger criteria directed to necessity and proportionality

- **Proposed section 27KC of the SDA (item 13 of Schedule 1) should be amended as follows:**
  - **paragraph 27KC(1)(b) should be amended to omit the reference to the issuance of the warrant being 'justified'. This should be substituted with a requirement that the issuance of the warrant must be 'reasonably necessary' to frustrate the commission of the offence(s) referred to in the warrant application; and**
  - **subsection 27KC(2) should include an additional mandatory consideration in applying the proportionality test. The issuing authority should be required to consider:**

[40] *Investigatory Powers Act 2016* (UK), paragraphs 102(1)(a) and 108(1)(a).

[41] *Human Rights Act 1998* (UK), paragraph 7(1)(a) and *Regulation of Investigatory Powers Act 2000* (UK), paragraph 65(2)(a) (prescribing the Investigatory Powers Tribunal as the 'appropriate tribunal' for the purpose of proceedings under the Human Rights Act in relation to actions of the intelligence services).

- **the specific nature of the proposed disruption activities to be carried out under the warrant;**
- **the proportionality of those activities to the suspected offending;**
- **the potential adverse impacts on non-suspects; and**
- **the steps proposed to be taken to avoid or minimise those adverse impacts, and their likely prospects of success.**

Issuing authority

89. Proposed subsection 27KA(2) provides that applications for data disruption warrants may be made to an 'eligible judge' or a 'nominated AAT member'. As noted above, these terms are defined in existing sections 12 and 13 of the SDA.

90. The definition of a 'nominated AAT member' in section 13 means that it will be open to the Attorney-General to appoint ordinary AAT members as issuing authorities for disruption warrants, provided they meet the relatively low eligibility requirement of attaining admission as a lawyer, in any Australian jurisdiction, for at least five years.

The need for judicial authorisation of data disruption warrants

91. The Law Council cautions against any attempt to justify the proposed approach on the basis of its consistency with existing provisions of the SDA for surveillance device and computer access warrants, which designate eligible judges and nominated AAT members as issuing authorities for those warrants.[42] In addition to the Law Council's strong reservations about the appropriateness of this model for any form of intrusive surveillance, it is unsuitable for powers of data disruption.

92. As the Richardson Review identified, data disruption activities are of a fundamentally different kind to electronic surveillance. Data disruption involves active intervention to frustrate the commission of an offence, by making it impossible (or at least more difficult) to carry out or continue the relevant criminal conduct. In contrast, electronic surveillance is carried out by law enforcement agencies for the purpose of investigating a suspected offence, by collecting admissible evidence that could be used to support the arrest, charge and prosecution of a suspect.

93. As the Richardson Review further identified, because data disruption is directed to active intervention as criminal acts are being carried out, it carries a significantly greater risk of causing collateral damage, loss or harm to non-suspects. This risk is aggravated by the fact that the relevant law enforcement agency will exercise its powers of data disruption on the basis of an uncontested assessment that a relevant offence has been committed, is being committed, or will be committed.

Appointment of superior court judges as the sole issuing authorities

94. The Law Council agrees with the Richardson Review that the extraordinary nature of data disruption activities, as opposed to surveillance for investigatory and evidence-collection purposes, must be reflected in the qualifications of the persons who may be appointed as issuing authorities for data disruption warrants. The Law Council concurs with the compelling position and supporting reasoning of the Richardson

[42] SDA, subsection 14(4) and section 16 (surveillance device warrants) and subsection 27A(7) and 27C (computer access warrants).

Review that only judicial officers, who are appointed (by consent) in their personal capacities, should be empowered to issue data disruption warrants.

95. Moreover, the Law Council considers that the gravity of data disruption powers means that only superior court judges—specifically judges of State and Territory Supreme Courts and the Federal Court of Australia—should be eligible for appointment as issuing authorities for disruption warrants. This will ensure that all applications to exercise extraordinary data disruption powers will be determined by a person of the highest seniority, standing and experience, including in complex legal and factual matters pertaining to investigative powers.

The importance of judicial issuing

96. Critically, a judicial officer is constitutionally bound to act judicially, not only when they are exercising a judicial power as a member of a court but also when they are exercising a power conferred *persona designata* (in a personal capacity). They must perform the relevant *persona designata* function 'in a just and fair manner, with judicial detachment'[43] and bring to bear the 'skill and experience of judicial officers'.[44] This means that judicial notions of independence, impartiality and procedural fairness would be required for all issuing decisions on data disruption warrants. It is also material that judicial officers have security of tenure, in sharp contrast to the fixed term appointments of AAT members, whose re-appointment for any subsequent terms is wholly reliant on executive discretion.

97. Moreover, the legal skills and experience of a judicial officer of a superior court, who is at the pinnacle of a long and distinguished career in the law, will generally far outweigh those of an AAT member who meets the minimum eligibility requirement as an Australian-admitted lawyer of five years' standing. In this respect, appointing judicial officers of superior courts, to the exclusion of ordinary AAT members, would be commensurate with the gravity of the proposed data disruption powers, and the extensive legal and factual complexity that is likely to be involved in determining warrant applications.

The case for limiting issuing authorities to superior court judges

98. Limiting issuing authorities for data disruption warrants to superior court judges will ensure that the public is given the strongest possible assurance that these extraordinary powers, which will be exercised on a covert basis, are subject to an independent and rigorous issuing process.

99. The importance of public trust and confidence—not merely a level of comfort among current and former 'insiders' within the law enforcement and intelligence communities, and the executive government more broadly with the present issuing arrangements—cannot be understated. It is public trust and confidence that gives moral legitimacy to the important work of security and law enforcement agencies, including the conferral and exercise of extraordinary powers. Both substantive and perceived independence are equally vital to the establishment and maintenance of that state of trust and legitimacy, especially when new powers are conferred, or existing powers are expanded.

100. In this respect, the observations of the former IGIS, that Australia is an 'outlier' compared to other jurisdictions in the Five Eyes alliance—all of which have

[43] *Love v Attorney-General (NSW)* (1990) 169 CLR 307 at [28] (per Mason CJ, Brennan, Dawson, Toohey and Gummow JJ).

[44] *Hilton v Wells* (1985) 157 CLR 57 at [13] (per Mason and Deane JJ).

implemented judicial authorisation models—has particular force.[45] That is, it would not be accurate to reduce the issue of international comparisons to one of attaining consistency for consistency's sake with Australia's international partners, or 'a solution in search of a problem'.[46] Rather, in assessing the value and significance of judicial authorisation—and in considering whether there is, in fact, a gap in Australia's legislative arrangements compared to those of like-minded countries—the material issue is identifying the means by which public trust and confidence in the extraordinary powers of security and law enforcement agencies can most effectively be established and maintained.

101. Further, an assessment of the appropriate model of authorisation should also take account of the recent, and continuing, trends towards significant and frequent legislative expansions of the scope and degree of intrusiveness of agency powers. Establishing a judicial authorisation model, constituted by superior court judges, would also be a valuable means of 'future-proofing' the means by which public trust and confidence can be maintained, as agencies' warrant-based powers are expanded in future (noting the present Bill is a prominent example of this practice).

102. As the former UK Independent Reviewer of Terrorism Laws, David Anderson QC (now Lord Anderson of Ipswich KBE QC), commented in his advisory report to the UK Government that endorsed the 'double lock' authorisation mechanism now enacted in the *Investigatory Powers Act 2016* (UK):

> *Public consent to intrusive laws depends on people trusting the authorities … This in turn requires knowledge at least in outline of what powers are liable to be used, and visible authorisation and oversight mechanisms in which the wider public, as well as those already initiated into the secret world, can have confidence.*
>
> *Trust in powerful institutions depends not only on those institutions behaving themselves (though that is an essential prerequisite), but on there being mechanisms to verify that they have done so. Such mechanisms are particularly challenging to achieve in the national security field, where potential conflicts between state power and civil liberties are acute, suspicion rife and yet information tightly rationed …*
>
> *Respected independent regulators continue to play a vital and distinguished role. But in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency: not just fashionable buzz-words, but the necessary foundation for the trust between government and governed upon which the existence of coercive and intrusive powers depends in a modern democracy.*[47]

103. For the former UK Independent Reviewer, judicial authorisation was an integral component of the procedural fairness, rights compliance and transparency that he identified as essential to public trust and confidence in the intrusive investigative

[45] See, for example: IGIS, *Supplementary submission to the PJCIS Review of the Australian Security Intelligence Organisation Legislation Amendment Bill 2020*, (November 2020), 2 and footnote 2.
[46] Richardson Review, Unclassified Report, Volume 2, (December 2019), 61 at [18.114].
[47] David Anderson QC, Independent Reviewer of Terrorism Legislation (UK), *A Question of Trust: Report of the Investigatory Powers Review,* (June 2015), 245-245 at [13.3]-[13.5].

powers conferred on the UK's security and law enforcement agencies.[48] As noted above, those powers include GCHQ's equipment interference warrants.

104. The Law Council considers that the UK Independent Reviewer's observations apply with equal force in the Australian context, including in relation to the proposed data disruption warrant regime in Schedule 1 to the Bill. Notably, in the UK, the persons responsible for issuing warrants under the IPA are judicial commissioners of the Investigatory Powers Commission. The eligibility requirements for appointment as a judicial commissioner are limited to persons who hold a judicial office that is the equivalent of a superior court in Australia, or a retired judge of such a court.[49]

105. Moreover, restricting issuing authorities to superior court judges is consistent with the recommendations of the Committee in its press freedoms inquiry, as accepted by the Government in December 2020, in relation to the issuing of investigatory warrants against journalists.[50] The Government endorsed the Committee's recommendation that issuing authorities for such warrants should be limited to superior court judges, in recognition of the sensitivities attending the criminal investigation of public interest journalism.[51]

106. Just as public interest journalism has been recognised as a category of case involving special sensitivities, which need to be reflected in the designation of issuing authorities for investigative warrants, so too is the exercise of an extraordinary power of disruption to actively and covertly frustrate the commission of an offence, for all of the reasons outlined by the Richardson Review (noted above).

Recommendation 5—superior court judges as sole issuing authorities

- **Proposed subsection 27KA(2) and related provisions of Schedule 1 to the Bill should be amended to provide that the issuing authority for a data disruption warrant is a judge of a superior court of record (specifically, a judge of a State or Territory Supreme Court or the Federal Court of Australia) who is appointed by the Attorney-General in their personal capacity.**

Specialisation and access to independent expertise by issuing authorities

107. The Law Council's primary position is that superior court judges, appointed *persona designata*, should be the sole issuing authorities for all warrants authorising the exercise of intrusive investigatory or intelligence powers, including data disruption.

108. However, the Law Council acknowledges that the third Independent National Security Legislation Monitor (**INSLM**), Dr James Renwick SC, made recommendations directed to building institutional arrangements to promote the specialisation of issuing authorities, and their access to independent technical expertise. These recommendations were made in the context of issuing authorities for the mandatory industry assistance orders under Part 15 of the *Telecommunications Act 1997* (Cth) given the limitation in the third INSLM's terms of

[48] Ibid, 285 at [1(c)] and subsequent recommendations in Chapter 15 on specific warrant-based powers.

[49] IPA, subsection 227(4) (persons holding 'high judicial office' as defined in subsection 60(2) of the *Constitutional Reform Act 2005* (UK), meaning a judge of the Supreme Court, Court of Appeal or High Court (and equivalent courts for Scotland and Northern Ireland).

[50] PJCIS, *Report on the inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*, (August 2020), 80-81 at [3.128]-[3.131] and recommendation 2.

[51] Australian Government, *Response to the PJCIS inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press,* (December 2020), 3-4. (While this document is dated 'October 2020' it was released publicly on 16 December 2020.)

reference to those orders. However, consideration could be given to expanding those arrangements to all warrant types.

109. The third INSLM recommended that there be independent issuing, by a new Investigatory Powers Division of the AAT, headed by a retired judge, comprising senior and experienced members with access to independent technical expertise.[52] The third INSLM was particularly concerned to establish a specialised body of institutional expertise in the determination of applications for these powers, as well as comprehensive physical, information and personnel security arrangements for the determination of those applications. He was also concerned to ensure that issuing authorities had visibility of all previous applications and decisions, including to avoid risks of oppression that may arise from overlapping or conflicting orders, or the combined impact of multiple powers.[53]

110. A Government response to the third INSLM's recommendations has not yet been released. The present Bill proposes to continue existing arrangements in respect of issuing authorities, without acknowledgement of the broader implications of the third INSLM's recommendations for other types of intrusive warrant-based powers, and associated powers to compel assistance in exercising those powers. The extrinsic materials do not provide insight into how this issue is being considered, and the Law Council queries whether the proposal in the Bill to replicate existing models of issuing warrants may impliedly represent a rejection of the third INSLM's recommendations, at least to the extent of any broader implications for multiple warrant types in addition to industry assistance orders.

111. In view of this uncertainty, the Law Council would support further consideration of the third INSLM's recommendations in the context of all warrant-based powers conferred on investigative and intelligence agencies, subject to one matter of qualification. As with some current and previous AAT appointments, the members of any new Investigatory Powers Division should only be superior court judges, who are appointed to that Division in their personal capacities. This would be the Law Council's preference for the composition of a specialist division of the AAT for the issuance of warrants authorising coercive and intrusive powers.

112. The Law Council emphasises that data disruption warrant applications (and any related applications for mandatory assistance orders) are likely to involve a comparable degree of factual, technical and legal complexity to requests for industry assistance orders under Part 15 of the Telecommunications Act. Accordingly, the Law Council suggests that any consideration of the third INSLM's recommendation to establish a dedicated Investigatory Powers Division of the AAT should also examine the possible extension of its functions to the issuance of data disruption warrants, among other types of investigatory powers.[54]

113. However, given the importance of judicial involvement in the issuing process, the membership of any new AAT Division should be limited to persons who also hold office as a superior court judge.

---

[52] Dr James Renwick SC, INSLM, *Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, (30 June 2020), Chapter 11 and recommendations 3-6.

[53] Ibid, 220-223.

[54] See further: Law Council of Australia, *Supplementary Submission to the PJCIS Review of the TOLA*, (August 2020), 8-10, in which the Law Council set out its full position on the third INSLM's recommendations. This included supporting the 'future proofing' of a new Investigatory Powers Division so that it could be invested with authorisation functions in addition to industry assistance notices.

Recommendation 6—an 'investigatory powers division' of the AAT

- **In the alternative to implementing the Law Council's recommendation 5 above, consideration should be given to implementing recommendations of the third INSLM in his review of the TOLA Act to establish an Investigatory Powers Division of the AAT, headed by a retired superior court judge.**
- **If the new Investigatory Powers Division is established, it should also be conferred with powers to issue data disruption warrants.**
- **Consistent with recommendations of the Law Council to the Committee's review of the TOLA Act, there should also be specific statutory eligibility criteria, and a transparent selection process, for all appointments to the new Investigatory Powers Division. The Law Council recommends that these members are superior court judges, who are appointed, in their personal capacities, as members of the new Division for the purpose of issuing warrants.**

The need for an effective contradictor in warrant applications

114. The task of determining data disruption warrant applications is likely to require complex judgments of fact and law. This will include in assessing the basis for the applicant's suspicion about the commission of a relevant offence or offences, and the likely effectiveness and proportionality of data disruption to the objective of frustrating the commission, or further commission, of such offences.

115. As noted above, particular complexities are likely to arise in the following tasks:

    - considering whether there are facts that may:
        - establish a defence or an exception to an offence; or
        - engage any applicable constitutional severance provisions that require an offence provision to be read down if a literal construction would infringe an express or implied constitutional limitation on Commonwealth legislative power;
    - assessing the likely effectiveness of technical disruption capabilities to frustrate the commission of offences; and
    - identifying potential impacts on non-suspects, and evaluating the effectiveness of proposed steps to avoid or minimise those impacts.

116. Given these complexities, and the significant risks that data disruption may have widespread and severe consequences for innocent third parties, it is important that issuing authorities have access to an effective and skilled contradictor. Such an approach would assist the issuing authority to review the information contained in the warrant application more thoroughly, and from more than one perspective.

117. By analogy, in August 2020, the Committee endorsed the need to create a regime of public interest advocates for all investigatory warrants sought in relation to journalists, in connection with secrecy offences. This recognised the significant sensitivities and adverse impacts on important national interests if such warrants were wrongly issued against journalists who were simply doing their jobs. That risk of error may be increased by the *ex parte* determination of a warrant application, without a sufficient mechanism to thoroughly test the matters alleged by the law

enforcement applicant.[55] The Government accepted the Committee's recommendation in December 2020.[56]

118. The Law Council considers that this reasoning applies with even greater force to applications for warrants authorising powers of data disruption to actively frustrate the commission of an offence, other than by exercising powers of arrest and charge.

119. As the Richardson Review cautioned, 'a poorly planned or executed operation could have disastrous implications, and may even compromise computers that support the provision of essential services, affecting the lives or livelihood of innocent people. All agencies, including the AFP, can and do make mistakes and this would be no exception'.[57] The effective and rigorous testing of applications, via an independent contradictor, would go a considerable way toward managing this risk, while also ensuring that operationally sensitive information remains protected from broader dissemination.

120. It will be important that the legislative requirements governing the appointment of public interest advocates ensure that only highly qualified and experienced persons, who are at arm's length from the executive government, are eligible for appointment. There will also need to be sufficient safeguards to ensure the independence of such advocates in performing their functions.

121. To satisfy these imperatives, the Law Council endorses the requirements recommended by the Committee in its press freedoms review, that such persons should be members of Senior Counsel or Queens Counsel, or a retired judge, and appointed by the Governor-General for a term of five years. Public interest advocates should be subject only to defined statutory grounds of removal for misbehaviour, infirmity or conflicts of interest.[58]

Recommendation 7—public interest advocates for data disruption warrants

- **Schedule 1 to the Bill should be amended to establish a regime of public interest advocates to act as contradictors in all applications for data disruption warrants.**
- **The eligibility requirements for appointment as a public interest advocate should be identical to those recommended by the Committee in its August 2020 press freedoms inquiry report (recommendation 2).**

Activities authorised under data disruption warrants

122. Proposed section 27KE sets out the acts that are authorised under a data disruption warrant. The Law Council has three main concerns with these provisions, namely:

- overbreadth and ambiguity in core concepts relevant to disruption, including:
  - the persons and computers that may be targeted; and
  - the meaning of 'data disruption' and the 'frustration' of an offence;

[55] PJCIS, *Report on the inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*, (August 2020), 83, recommendation 2.

[56] Australian Government, *Response to the PJCIS inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press,* (December 2020), 3-4.

[57] Richardson Review, *Unclassified Report,* Volume 3 (December 2019), 220 at [38.68].

[58] PJCIS, *Report on the inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*, (August 2020), 83, recommendation 2 (bullet point 4).

- the conferral of a power to cause material loss or damage to lawful computer users where 'justified and proportionate', and a lack of transparency and external supervision in making that assessment; and

- the repetition of several problems in existing provisions governing computer access warrants for law enforcement agencies and ASIO, as enacted by the TOLA Act in 2018. These issues were raised by the Law Council and other stakeholders, including the IGIS, during the multiple inquiries undertaken by the Committee and the third INSLM into the TOLA measures. They principally concern areas of overbreadth, ambiguity and inadequate oversight and accountability mechanisms in relation to powers to:
  - intercept telecommunications for the purpose of doing any act or thing that is authorised under the warrant (including but not limited to gaining access to data held in, or accessible from, a computer);
  - remove computers and other things from premises;
  - use force against persons for the purpose of executing the warrant; and
  - conceal the fact that an act or a thing has been done under the warrant, including after that warrant has ceased to be in force.

Breadth of 'target computers' and persons subject to powers under warrants

123. As noted above, under proposed subsection 27KA(1), data disruption warrants would be issued to disrupt data that is held in a computer (the 'target computer') for the purpose of 'frustrating' the commission of a 'relevant offence'. This is provided that the acts constituting the suspected 'relevant offence' involve, or are assessed as being likely to involve, data held in the target computer.

Component terms 'computer' and 'data held in a computer'

124. The component terms 'computer' and 'data held in a computer' are defined in existing section 6 of the SDA in a manner that significantly extends their ordinary meanings, as follows:

- ***'computer'*** means all or part of:
  - one or more computers;
  - one or more computer system;
  - one or more computer networks; or
  - any combination of the above; and
- the expression ***'data held in a computer'*** extends the ordinary meaning of that phrase to cover data that is held in a removable data storage device, where the device is:
  - temporarily held in a computer (for example, a USB drive that is plugged into a laptop or a PC); or
  - connected to a computer network (for example, a wireless external hard drive that is connected to the internet or a local area network via WiFi).

Identification of a 'target computer' in a warrant

125. Proposed subsection 27KA(6) further provides that the 'target computer' specified in a data disruption warrant may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises; or

(c) a computer associated with, used by, or likely to be used by, a person, whose identity may or may not be known. (The expression 'person' is defined in subsection 2C(1) of the *Acts Interpretation Act 1901* (Cth) as covering an individual, a body corporate and a body politic.)

Implications for the scope of individual data disruption warrants

126. The combination of these broad terms means that a **single** data disruption warrant will authorise, or will be capable of authorising, the following activities:

- data disruption and related activities in relation to a very large, and potentially unquantifiable, number of:
  - offences whose commission is sought to be frustrated via the disruption of data. That is, all offences of the 'kind' specified in the warrant, which can be any Commonwealth or federally relevant State offence punishable by three or more years' imprisonment, or any other offence prescribed by regulation. This includes future offences that are suspected of being likely to occur, or about to occur;
  - individual computer devices, such as:
    - multiple devices which are each connected to a common network, such as a local area network belonging to a company or educational institution; and
    - multiple devices which are each immediately connected to a different network, but those networks are connected to each other (as is the case with devices connected to the internet); and
  - individual persons, where the target computer is specified under proposed paragraph 27KA(6)(c) as being one that is associated with, or likely to be used by, a body corporate or a body politic; and
- repeated instances of data disruption, and other acts authorised under section 27KE, in relation to the broad range of offences, devices and persons mentioned above while the warrant is in force. This may be a protracted period of time, of up to 90 days (subject to extension for up to a further 90 days, or 180 days in total). Further, even if a data disruption warrant expires without extension, there is no cap on the number of subsequent warrants that can be issued on the same grounds.

More stringent requirements should apply to data disruption than data access

127. The Law Council acknowledges that equivalent definitions are currently used in the legislative frameworks governing law enforcement and ASIO computer access warrants, in Division 4 of Part 2 of the SDA and section 25A of the ASIO Act.

128. However, data disruption is a fundamentally different type of activity to accessing data held on, or from, a computer. Disruption carries greater risks of adversely affecting innocent third parties who use, or otherwise rely upon, the operation of computers that may be affected collaterally (whether intentionally or otherwise).

129. The Law Council considers that the fundamentally different nature of data disruption as compared to data access should be reflected in all aspects of the statutory framework for data disruption warrants. In particular, it should be reflected in:

- precision of terminology;
- acts able to be authorised under data disruption warrants, including the permitted purposes and scope of those activities;
- issuing thresholds and process (including issuing authorities);
- maximum duration (including extension and subsequent warrants directed to the same or substantially similar matters);
- permitted uses and admissibility of information obtained in the course of performing data disruption activities; and
- oversight, reporting and review requirements.

130. This guiding principle informs the Law Council's recommendations in relation to the specific matters discussed below.

Meaning of 'disruption' of data and 'frustration' of offences

'Disruption'

131. As the Richardson Review observed, the ordinary meaning of the term 'disruption' in relation to data held in a computer has the potential to be 'nebulous'[59] unless it is defined clearly in primary legislation. However, the Bill does not contain a definition of 'disruption' in relation to such data, even on an inclusive or illustrative basis.

132. Nor does the Bill require each data disruption warrant request to specify the particular acts of disruption, or at least the types of acts, that are sought to be carried out under the warrant. Consequently, there is no requirement for the issuing authority for a data disruption warrant to specifically approve identified acts of data disruption. Unless an individual issuing authority decided to impose warrant-specific conditions that only authorised specified acts of data disruption under a warrant they have issued, then the selection of the particular acts of data disruption would be left wholly to the discretion of the AFP and ACIC in executing the warrant.

133. In this event, the warrant instrument would simply provide a wholesale authorisation of any or all acts that are capable of being characterised as 'data disruption', in the absence of any statutory guidance or direction about the meaning of that term.

'Frustration'

134. Similarly, the concept of 'frustration' in relation to the commission of an offence is not defined for the purpose of the proposed data disruption warrant regime. The intended scope and limits of this term are unclear in the novel context of data disruption powers in relation to cyber-enabled offences that have occurred, are occurring, or are about to occur, or are likely to occur in future.

135. The ambiguity in the concept of 'frustration' is especially problematic for data disruption warrants that are issued in respect of 'relevant offences' that have already been committed, as would be permitted by proposed paragraph 27KA(1)(a). Is the concept of 'frustration' in this context intended to mean making any further commission of the same offence, or a similar type of offence, impossible? Or is the concept of 'frustration' intended to limit the harmful impacts of the completed offence, and prevent the offender from achieving an underlying criminal purpose, such as deriving profit or another benefit?

136. In addition, it is unclear whether the concept of 'frustration' in relation to a suspected offence that is occurring, or is about to occur, would extend to acts of data disruption

[59] Richardson Review, *Unclassified Report*, Volume 3, (December 2019), 220 at [38.66].

which only minimise the resultant harm, rather than making the apprehended commission of the offence impossible. It is foreseeable that, in some circumstances, it may be technically impossible to prevent the commission of a cyber-enabled offence, but it may be possible to mitigate or minimise its impacts.

137. For example, in the case of an offence in the nature of using the internet to disseminate child sexual abuse material, would the concept of 'frustration' cover data disruption activities that resulted in that material only being accessible to a much smaller number of persons than the intended recipients? This may occur if a data disruption activity was carried out after unlawful content was found on a web-based platform, and once the data disruption activity was complete, that content and the platform upon which it is hosted would be inaccessible to any further users.

Recommended amendments

138. The Law Council considers that stronger statutory parameters are required for the concepts of 'disruption' and 'frustration', so that there is clarity and certainty for issuing authorities, warrant applicants, executing officers and the wider community about the scope and limits of the attendant data disruption powers. Efforts should be made to craft statutory definitions of these terms, which could be on an inclusive (non-exhaustive) basis if necessary.

139. However, if it is considered that it would not be feasible to impose statutory definitions of universal application, then the legislation should require individual warrant requests and issuing decisions to contain a greater level of specificity about the data disruption activities being authorised. In particular, there should be an express requirement in proposed paragraph 27KA(3)(b) for the statement of facts and grounds that must accompany every warrant application to particularise:

- the acts or types of acts of data disruption that are proposed to be carried out under the warrant;
- the anticipated or desired impact of those acts on the commission or of the relevant offence; and
- the likelihood that the proposed acts of data disruption will achieve that outcome.

140. This would at least provide clarity to the issuing authority, on a case-by-case basis, of the specific disruption activities they are being requested to authorise, rather than leaving this solely to the discretion of the law enforcement officers responsible for executing the warrant, if issued. However, the inclusion of statutory definitions would be a preferable approach because it would facilitate certainty and consistency across all data disruption warrants.

Recommendation 8—statutory definitions of 'disruption' of data and 'frustration' of the commission of an offence

<u>Preferred option</u>

- **Schedule 1 to the Bill should be amended to insert definitions of the concept of 'disrupt' (in relation to data) and 'frustrate' (in relation to the commission of an offence) for the purpose of the proposed data disruption warrant regime. Such definitions could be drafted on an inclusive basis, if necessary.**
- **Amendments to the Bill should be circulated before the Bill is scheduled for debate. The Committee should be requested to review and report to Parliament on those amendments prior to any debate.**

Alternative (non-preferred) option

- **Proposed paragraph 27KA(3)(b) (item 13 of Schedule 1) should be amended to provide that the statement of facts and grounds accompanying all applications for data disruption warrants must specify the following matters:**
  - **the acts or types of acts of data disruption that are proposed to be carried out under the warrant;**
  - **the anticipated impacts of those specific acts or types of acts of disruption on the commission of the relevant offence (that is, how they are intended to frustrate that offence); and**
  - **the likelihood that the relevant acts or types of acts of disruption will achieve that objective.**

Causation of material loss or damage to lawful computer users

141. Proposed paragraph 27KE(7)(a) of the SDA replicates equivalent provisions for computer access warrants under the SDA and ASIO Act.[60] It limits the authority to do an act or thing under a data disruption warrant that is likely to cause material interference with, or interruption or obstruction of:

    - a communication in transit. That is, a telecommunication passing over the Australian telecommunications network, within the meaning of the *Telecommunications (Interception and Access) Act 1979*) (Cth) (**TIA Act**); or
    - the lawful use of a computer by persons who are not suspects in relation to the suspected offence or offences.

142. Such acts are only authorised where they are necessary to do one of the things specified in the warrant. The Law Council supports the test of necessity rather than a lower threshold of mere assistance, convenience or utility of any degree.

143. However, proposed paragraph 27KE(7)(b) contains a major departure from equivalent provisions under the computer access warrant regimes for law enforcement agencies and ASIO in the SDA and ASIO Act. It expressly authorises the AFP or ACIC to do acts or things under a warrant that cause material loss or damage to persons lawfully using a computer, where that loss or damage is 'justified and proportionate, having regard to the offences covered by the warrant'.

144. In contrast, the computer access warrant provisions of the SDA and ASIO Act categorically prohibit any acts which are likely to have such results. It is immaterial that the AFP, ACIC or ASIO (as applicable) may consider that the causation of such loss or damage is necessary to execute the warrant.[61]

145. The Law Council has several concerns with the proposal to authorise the AFP and ACIC to cause material loss, damage to lawful computer users who are not suspects in relation to the offence or offences covered by a data disruption warrant. These matters are discussed below and, in summary, are that:

    - the necessity of the power has not been demonstrated;

[60] SDA, paragraph 27E(5)(a) and ASIO Act, paragraph 25A(5)(a).
[61] SDA, paragraph 27E(5)(b) and ASIO Act, paragraph 25A(5)(b).

- the thresholds for the exercise of the power are disproportionately low to the gravity of its impacts on individual rights and liberties;
- there is overbreadth in the purposes for which the power may be exercised, in that the AFP and ACIC may cause material loss or damage for the purpose of carrying out any activity under the warrant, not only data disruption;
- the conferral of the power to cause material loss or damage to lawful computer users would, as the Richardson Review cautioned, place law enforcement officers in the role of 'judge, jury and executioner' in relation to decisions about whether to extinguish or significantly infringe the private property rights of non-suspects;
- the conferral of a broad power to cause material loss or damage to lawful computer users under data disruption warrants, and the prohibition on such activities under computer access warrants, may create propriety risks for the AFP and ACIC in selecting the particular type of warrant to be used in the investigation of cyber-enabled offences; and
- if the AFP or ACIC requested ASD to carry out a disruption activity under a data disruption warrant that has been issued to the AFP or ACIC, there may be a mismatch in the scope of multiple statutory immunities that would apply to ASD staff members in these circumstances. An ASD staff member may have a wider immunity in relation to acts done under data disruption warrants than they would if they had done the same acts for the purpose of performing ASD's own functions under paragraph 7(1)(c) of the *Intelligence Services Act 2001* (Cth) (**ISA**) to prevent and disrupt cybercrime outside Australia, via electronic means.

Inadequate justification of necessity

146. The Law Council is concerned that the Explanatory Memorandum offers no clear or targeted justification for authorising, and therefore conferring immunity on the AFP and ACIC for, acts that are likely to cause material loss or damage to lawful computer users under proposed paragraph 27KE(7)(b).

147. The Explanatory Memorandum states that 'prohibiting the ability to interact with a third-party's data altogether may critically hinder the ability to frustrate the commission of offences as third-party data can often be inextricably linked or associated to the target computer or the data needing to be accessed'. It provides an example of disruption of the operation of a computer server that hosts a child exploitation forum, together with lawful data storage by third parties. It states that disrupting the operation of that server, and thereby preventing both the lawful and unlawful users from accessing data, 'may be deemed justifiable and proportionate' in particular factual circumstances.[62]

148. However, this example appears to be limited to acts that cause material interference, interruption or obstruction to lawful computer use by non-suspects, which is separately regulated under proposed paragraph 27KE(7)(a) and applies a higher threshold of necessity. It does not address the proposed power to cause material loss or damage under proposed paragraph 27KE(7)(b), which applies the lower threshold of 'justifiable and proportionate'.

149. The power to cause material loss or damage to non-suspects is highly intrusive, and therefore its necessity and proportionality requires comprehensive and detailed

[62] Explanatory Memorandum, 38 at [116]-[117].

justification. Given the absence of such justification in the extrinsic materials to the Bill, the Law Council submits that the measure should not proceed.

Disproportionately low threshold for exercising the power

150. The power to cause material loss or damage to third parties who are not under any suspicion of wrongdoing is not subject to a threshold of necessity. Rather, it is subject to a lower, and potentially more subjective, threshold of whether the causation of such loss or damage is 'justifiable' or 'proportionate'. This will necessarily require a case-by-case assessment by the officers executing a data disruption warrant, based on the circumstances known to them at the time.

151. The extrinsic materials to the Bill provide no justification as to why such an extraordinary power should not be a last resort, where it has been established that any other methods of carrying out a data disruption activity would be ineffective, or at least materially less effective. A threshold of necessity would reflect the significant nature of the power, including the extinguishment of the legal rights of those third parties to compensation and other remedies for loss or damage. It would also give legal effect to the statement of policy intent in the Explanatory Memorandum that causing material loss or damage to a third-party computer user, who is acting lawfully, 'is not the overall intent' of the proposed disruption warrant regime.[63] That intention is not presently reflected in the substantive provisions of the Bill.

152. Moreover, the Explanatory Memorandum contains no justification for the proposal to apply a lower threshold for the authorisation given in proposed paragraph 27KE(1)(b) for the causation of material loss or damage, as compared to the threshold of necessity in proposed paragraph 27KE(1)(a) for the causation of material interruption, interference or obstruction with the lawful use of a computer. The Law Council considers this disparity is illogical and potentially arbitrary. Acts which cause material loss or damage are likely to have a significantly greater and more protracted effect on non-suspects who are lawfully using computers. It follows that such acts should be subject to at least an equal or a higher threshold.

Disproportionately broad scope of the power

153. The limited justification provided in the Explanatory Memorandum suggests that the power to cause material loss or damage to non-suspects is intended to be exercised for the purpose of carrying out a data disruption activity under a warrant.

154. In fact, proposed paragraph 27KE(7)(b) has a much broader application. It authorises the causation of material loss or damage to non-suspects for the purpose of doing **any thing** authorised under a warrant. This includes all of the matters specified in subsections 27KE(2) and (8) such as:

- entering and exiting premises on private property;
- temporarily removing computers and other things from premises;
- intercepting telecommunications for the purpose of doing any thing authorised under the warrant (not only accessing relevant data, or disrupting data);
- connecting electronic equipment to a computer (an individual device or a network) and using it to gain access to data or disrupting data; and
- copying data for the purpose of determining whether it is covered by the data disruption warrant.

[63] Ibid at [117].

155. The Explanatory Memorandum does not acknowledge the breadth of the purposes for which the AFP and ACIC would be authorised to cause material loss or damage to non-suspects who are lawfully using a target computer, or another computer. Consequently, it does not offer any explanation of the necessity or proportionality of the power (and attendant immunity) for purposes additional to carrying out a data disruption activity. The breadth of the power to cause material loss or damage to non-suspects aggravates the Law Council's concerns about the disproportionately low threshold for its exercise (as outlined above). In the absence of compelling justification, this power should be removed. At the very least, its scope should be limited to data disruption activities alone.

Law enforcement officers as 'judge, jury and executioner'

156. As the Richardson Review cautioned, the conferral of a disruption power that authorises law enforcement agencies to cause material loss or damage to non-suspects effectively authorises those agencies to act as 'judge, jury and executioner' in deciding whether to carry out those acts.

157. The authorisation framework proposed in Schedule 1 to the Bill aggravates the concerns expressed by the Richardson Review, due to the breadth of the 'relevant offences' in respect of which data disruption warrants may be issued; the absence of authorisation by superior court judges alone; and the low threshold for authorising acts that are likely to cause material loss or damage to a third-party who is lawfully using a computer.

158. In addition, individual law enforcement officers will be responsible for making the assessment of whether the proposed act is 'justifiable and proportionate', and therefore permissible, having regard to the relevant offence sought to be frustrated. As noted above, individual law enforcement officers will also be responsible for making assessments as to whether a particular suspected offence is of the same 'kind' as the offence or offences specified in a disruption warrant, and assessing the availability of exceptions, defences or constitutional severance provisions. Such decisions will conceivably be made in circumstances of significant urgency.

159. The Law Council is concerned that these highly significant decisions, with major adverse consequences for non-suspects, will not be subject to external, prior approval. Rather, they will only be subject to *ex post facto* advisory oversight by the Commonwealth Ombudsman. The Government would not be obliged to accept or implement any recommendations of the Ombudsman, including to pay compensation to aggrieved persons who have suffered material loss or damage as a result of data disruption activities carried out under a warrant.

160. Moreover, an aggrieved individual may have significant difficulty in accessing the necessary evidence to commence civil proceedings for damages, on the basis that the AFP or ACIC acted outside the scope of a disruption warrant because they incorrectly applied the 'justified and proportionate' assessment in proposed paragraph 27KE(7)(b). In any event, such proceedings may be prohibitively expensive for a party that has already suffered major loss or damage.

161. It should also be noted that Australia lacks an equivalent specialist adjudicative body to the Investigatory Powers Tribunal in the UK, which is empowered to determine challenges to investigatory powers warrants, including equipment interference warrants under the IPA.[64] The Investigatory Powers Tribunal has special procedures for taking classified evidence and issuing public decisions. This includes an ability to proceed on the basis of 'assumed facts' that do not require a security agency to

[64] *Regulation of Investigatory Powers Act 2000* (UK) (**RIPA**), Part IV.

confirm or deny the existence of particular operational activities. Rather, the Investigatory Powers Tribunal makes decisions on application of the law to the assumed facts, and publishes its judgments on that basis.[65] Importantly, it also has jurisdiction to determine applications made under the *Human Rights Act 1998* (UK), as well as complaints made under the *Regulation of Investigatory Powers Act 2000* (UK) alleging that an investigative agency has acted unlawfully.[66]

Propriety risks in selection of warrant type

162. The Law Council is also concerned that the authorisation for acts which cause material loss or damage in proposed paragraph 27KE(7)(b) may create propriety risks for the AFP and ACIC in making decisions about whether to seek a data disruption warrant, or a computer access warrant, in relation to the suspected commission of a cyber-enabled offence.

163. This reflects that both data disruption warrants and computer access warrants would authorise the AFP or ACIC to access data that is held in, or is accessible from, a computer. Information obtained under both types of warrants would be admissible as evidence in a subsequent criminal prosecution or civil proceedings, such as applications for confiscation orders under proceeds of crime laws.

164. However, a data disruption warrant will also authorise the commission of acts or things that are likely to cause material loss or damage to non-suspects who are lawfully using a computer, where this is self-assessed by the AFP or ACIC officers executing the warrant as being 'justified and proportionate' for the doing of any act or thing authorised by the warrant. This is not limited to the specific act or acts of data disruption, and can extend to other activities such as entering premises, or temporarily removing computers or other things from premises. In contrast, existing paragraph 27E(5)(a) of the SDA provides that computer access warrant do not, in any circumstances, authorise acts which are likely to cause material loss or damage to lawful computer users.

165. Consequently, there is a risk that data disruption warrants could effectively be preferred over computer access warrants, because of the ability to cause material loss or damage to third parties—as well as having access to a discretionary power to frustrate the commission of the offence by disrupting data—even though there is an intention to seek the arrest and charge of suspects in relation to the 'relevant offences'.

Ambiguities in the interaction of proposed ss 27KE(7)(b) and 27KE(12)

166. In addition, it is unclear how the authorisation under proposed paragraph 27KE(7)(b) will interact with the limitation in proposed subsection 27KE(12). The latter provision states that a data disruption warrant must not be executed in a manner that:

    (a) results in loss of or damage to data, unless the loss or damage is justified and proportionate, having regard to the offence or offences covered by the data disruption warrant;

    (b) causes a person to suffer a permanent loss of:

        (i) money;

        (ii) digital currency; or

[65] Ibid, section 68. See also: Investigatory Powers Tribunal, *Closed and Open Procedures*, website, < https://www.ipt-uk.com/content.asp?id=13> (November 2016).

[66] RIPA, section 65.

(iii) property (other than data).

167. The absolute prohibition specified in paragraph 27KE(12)(b) on causing permanent loss of money or property other than data is difficult to reconcile with the conditional authorisation and immunity conferred in proposed paragraph 27KE(7)(b) in relation to acts that cause material loss or damage to lawful, third-party computer users who are not suspects, where this is assessed by the AFP or ACIC members executing the warrant as justified and proportionate.

168. In particular, it unclear whether the following activities would be permitted under proposed paragraph 27KE(7)(b) or prohibited under proposed paragraph 27KE(12)(b):

- **loss of income,** where acts done under a data disruption warrant prevent a non-suspect from lawfully using a computer network or system to access data that is necessary to conduct their business or personal affairs, and that third-party loses their ability to derive an income for a period of time (such as acts which prevent a lawful online business from trading). The loss of income that would otherwise lawfully have been earned during a period of time amounts to a permanent loss of money. It is therefore unclear whether proposed subparagraph 27KE(12)(b)(i) or (ii) would prohibit such an act, or whether proposed paragraph 27KE(7)(b) would conditionally permit it, if it is assessed as 'justified and proportionate' in the circumstances; and
- **loss of functionality**, where acts done under a data disruption warrant do not cause physical damage to a computer, such as a laptop or PC, or physical network infrastructure, but renders it permanently inoperative or permanently impairs its operation. This would deprive non-suspects of the ability to use their property. The extinguishment of rights to use property for its intended purpose could arguably be characterised as a form of 'destruction'. It is therefore unclear whether proposed subparagraph 27KE(12)(b)(iii) would prohibit an act causing such a result, or whether proposed paragraph 27KE(1)(b) would conditionally permit it, if it is assessed by the persons executing the warrant as 'justified and proportionate' in the circumstances.

169. While the Explanatory Memorandum states that proposed subsection 27KE(12) is intended to be 'distinct from' proposed subsection 27KE(7), it does not explain the intended interaction of the two provisions, with respect to acts that are likely to cause, and in fact cause the following forms of loss in relation to property rights:

- financial loss to non-suspects who are lawfully using a computer; or
- the effective extinguishment of the property rights of a person who owns or leases a computer, by rendering that computer inoperative.[67]

170. To avoid ambiguity and uncertainty in relation to the legal status of acts that may cause serious financial loss, or effectively extinguish intangible property rights in relation to physical property, the Bill should be amended to address this matter.

171. It may be that proposed subparagraphs 27KE(12)(b)(i) and (ii) are intended only to prohibit acts or things that result in the permanent seizure of physical or digital currency from a person's online bank account. Without such a prohibition, disruption warrants could effectively operate as a 'backdoor' alternative to law enforcement agencies seeking and obtaining forfeiture orders under applicable proceeds of crime legislation. However, if that is the subjective policy intent, then it

[67] Explanatory Memorandum, 41 at [129].

should be given explicit effect in the Bill, to avoid any doubt about the scope of the prohibition.

172. Similarly, if proposed subparagraph 27KE(12)(b)(iii) is intended only to prohibit acts which result in the permanent seizure or physical destruction of a chattel (to the exclusion of rendering it inoperative, thereby extinguishing a person's intangible rights to make use of that physical property), then this should be made explicit on the face of the provision of Schedule 1 to the Bill, to avoid any doubt.

173. Irrespective of the subjective policy intent, proposed paragraphs 27KE(7)(b) and 27KE(12)(b) should be amended to remove doubt about their respective scope and interaction. In their present form, these provisions fail to provide adequate clarity and certainty for law enforcement agencies executing data disruption warrants, and non-suspects who may suffer significant loss or damage as a result of acts done under those warrants. Given the gravity of the consequences of disruption activities, a higher degree of legal certainty is necessary.

Interaction with separate statutory immunities for ASD under the Criminal Code

174. The unclassified report of the Richardson Review and earlier public remarks of the Minister for Home Affairs about the potential involvement of ASD in data disruption activities appear to identify a possibility that staff members of ASD could (at the discretion of the AFP or ACIC) be called upon to execute at least some of the data disruption warrants are issued to the AFP or ACIC, if these powers are conferred.[68]

175. This means that ASD staff members would be authorised, under those warrants, to do acts or things which cause material loss, damage or interference to lawful computer users (including non-suspects) if those acts are 'justified and proportionate'.[69]

176. There are two different legal mechanisms by which ASD staff members could execute the data disruption component of these warrants. However, each mechanism would enliven a separate source of statutory immunity, which have differences in their respective scope and limits. The two legal mechanisms are as follows, with their respective implications for immunities detailed below:

- the involvement of ASD staff members could be supported by ASD's statutory functions under paragraph 7(1)(f) of the *Intelligence Services Act 2001* (Cth) (**ISA**) to cooperate with another Commonwealth agency for the purpose of that other agency performing its own functions. This is provided that the other Commonwealth agency is prescribed in regulations made under section 13A of the ISA. This mechanism would therefore require the making of regulations to prescribe the AFP and ACIC, as no such regulations are in force; or
- the individual ASD staff members could be seconded to the AFP or ACIC for the warrant operation, meaning they would be members of the AFP or ACIC.

Immunities if s 7(1)(f) of the ISA applied

177. If the statutory framework for cooperation under paragraph 7(1)(f) and section 13A of the ISA is engaged to enable staff members of ASD to execute the AFP or ACIC's data disruption warrants, then a staff member of ASD who does an act or a thing

[68] Richardson Review, *Unclassified Report*, Volume 3 (December 2019), 216-218 and 221 and recommendation 162. See also: The Hon Peter Dutton MP, Minister for Home Affairs, *Transcript of joint press conference with the Prime Minister*, Parliament House, Canberra, 6 August 2020.

[69] Bill, Schedule 2, item 13 (inserting proposed paragraph 27KE(7)(b) of the SDA).

under such a warrant will be taken to have done so in the course of performing the functions of ASD (not the AFP or ACIC).

178. This means that the ASD staff member would be covered by the civil and criminal immunity in section 14 of the ISA for acts done in the 'proper performance' of ASD's functions. They would also likely be covered by a civil and criminal immunity in section 476.5 of the Criminal Code for certain computer-related activities done in the 'proper performance' of ASD's functions. (It should be noted that another Bill presently under review by the Committee proposes to expand the immunity in section 476.5 of the Criminal Code to cover further computer-related actions that were done inside Australia.)[70]

179. It is possible that the broad concept of acts done in the 'proper performance' of ASD's functions could cover some instances of technical non-compliance with the legal limits of authority under a warrant (for example, where there was a genuine but mistaken belief that an act was authorised under a warrant, when in fact it was not).

Protections if ASD staff members were seconded to the AFP or ACIC

180. However, if ASD staff members were seconded to the AFP or ACIC for the purpose of executing a data disruption warrant, they would be reliant on a narrower source of protection. This would be one or both of the following:

- the general defence of 'lawful authority' in section 10.5 of the Criminal Code, in respect of acts and things done under the authority of the warrant (therefore excluding acts done in purported compliance which, in fact, exceeded the limits of authority); and

- the application provision in subsection 476.2(4) of the Criminal Code for the purpose of the computer offences in Part 10.7 of the Criminal Code in relation to unauthorised access to or interference with computers. It states that a computer-related act is taken not to be 'unauthorised' (for the purpose of the physical elements of computer offences) if it was done under the authority of a warrant issued under an Australian law. This would only effectively immunise the activities of an ASD staff member that were done in strict compliance with the limits of authority under a warrant.

The need for clarity about the nature and legal basis for ASD involvement

181. Given the potentially significant difference in the source and scope of immunities for ASD staff members and the proposal for data disruption warrants to authorise material loss or damage to lawful computer users, it is important that the legal basis for any such involvement is clarified.

182. The Law Council submits that, if an ASD staff member is called upon to execute a data disruption warrant issued to the AFP or ACIC, they should be governed solely by the immunity in subsection 476.2(4) of the Criminal Code. That is, they would only have protection from legal liability in respect of acts done in strict compliance with the limits of authority under the warrant.

183. There should be no legal possibility for ASD staff members to be covered by the broader immunities in section 14 of the ISA and section 476.5 of the Criminal Code (for acts done in the 'proper performance' of ASD's functions).

[70] Security Legislation Amendment (Critical Infrastructure) Bill 2020, Schedule 2.

184. If there was an ability for ASD staff members to have a broader immunity for acts done in the execution of a data disruption warrant than ordinary members of the AFP or ACIC, this may create a perverse incentive for ASD to be, in effect, the *de facto* executing agency for those warrants.

185. The Law Council recommends that Division 476 of the Criminal Code and section 14 of the ISA should be amended to make this explicit. That is, even if regulations were made under section 13A of the ISA to list the AFP and ACIC as agencies with which ASD may perform its cooperation function in paragraph 7(1)(f) of the ISA, the attendant legal protection for cooperation that comprises executing data disruption warrants is limited to acts done in strict compliance with the limits of authority under the warrant, as is the case for AFP and ACIC staff members.

Recommendation 9—removal or limitation of authority to cause material loss or damage to third-party, lawful computer users

Preferred option

- **In the absence of evidence justifying the necessity of proposed paragraph 27KE(7)(b) (item 13 of Schedule 1), this provision should be omitted from the Bill.**
- **It should be substituted with an absolute prohibition on the AFP and ACIC doing acts or things that are likely to cause material loss or damage to third-party computer users, who are not suspects or persons of interest in an investigation or operation.**

Alternative (non-preferred option)

- **If the Committee is satisfied that data disruption warrants should authorise the AFP and ACIC to do acts or things that are likely to cause material loss or damage to non-suspects who are lawfully using computers, the Bill should be amended as follows, in addition to implementation of the Law Council's previous recommendations:**
  - **the authorisation conferred under proposed paragraph 27KE(7)(b) should be subject to a higher threshold, being that of necessity (not merely 'justified and proportionate');**
  - **the authorisation conferred under proposed paragraph 27KE(7)(b) should be limited to acts of data disruption done under the warrant, and acts that are directly preparatory or incidental to data disruption. It should not apply to any or all of the acts or things authorised under the warrant (such as entry to premises, access to data, or the temporary removal of computers or things from premises);**
  - **the AFP and ACIC should be subject to specific obligations to provide particulars in their warrant applications about:**
    - **the likely impacts of all acts done under the warrant on non-suspects who are lawfully using a computer;**
    - **the steps that will be taken to avoid or minimise those impacts; and**
    - **the likely effectiveness of those steps in avoiding or minimising the likely impacts on non-suspects.**

- **the AFP and ACIC should be required to notify the Commonwealth Ombudsman if any acts or things are done in purported reliance on a data disruption warrant, which are likely to cause material loss or damage to third-party computer users. Notification must be given as soon as possible after the AFP or ACIC becomes aware of the likely impacts on third parties;**
- **the AFP and ACIC should be required to include information in their annual reports (at least on a classified basis) about the circumstances in which they have relied on the authority of proposed paragraph 27KE(7)(b) to engage in activities which are likely to cause material loss or damage to non-suspects; and**
- **the Bill should also make consequential amendments to Division 476 of the Criminal Code and section 14 of the ISA, to ensure that:**
  - **ASD staff members are treated identically to AFP, ACIC and ASIO officials under subsection 476.2(4) of the Criminal Code, when ASD staff members are executing data disruption warrants for the AFP or ACIC. (That is, these staff members will have lawful authority, and therefore immunity, when acting within the limits of authority under a data disruption warrant); and**
  - **the broader immunity in section 476.5 of the Criminal Code, which could potentially cover acts of ASD staff members that exceeded the limits of authority under a data disruption warrant, will not apply to the actions of ASD staff members in executing data disruption warrants.**

Telecommunications interception

186. Proposed paragraph 27KE(2)(h) of the SDA provides that a disruption warrant authorises the interception of telecommunications, for the purpose of doing any act specified in the warrant. It replicates equivalent provisions for law enforcement and ASIO computer access warrants, as inserted by the TOLA Act in 2018.[71]

Overbreadth in the purposes for which interception activities can be carried out

187. As the Law Council noted in its submissions to the multiple pre-enactment and post-enactment reviews of the TOLA legislation, the scope of the power to intercept telecommunications under the SDA and ASIO Act is broader than the stated objective that ASIO and law enforcement agencies need to intercept telecommunications in order to gain access to data that is held in, or is accessible from, a computer. (For example, where computer access and network exploitation activities are carried out using an internet connection.)[72]

188. The Law Council acknowledges that certain acts of data disruption, such as those carried out using an internet connection, may require the incidental interception of telecommunications. However, no cogent justification has been advanced for a power to intercept telecommunications for the purpose of the wide range of other

[71] SDA, paragraph 27E(2)(h); ASIO Act, paragraph 25A(4)(ba).

[72] See, for example, Law Council, *Supplementary submission to the PJCIS Review of the TOLA Act*, (August 2020), Attachment 1, 19-20 and 24 (citing previous submissions to the PJCIS Review of the TOLA Bill and the Third INSLM Review of the TOLA Act).

activities that can be authorised under a data disruption warrant, such as gaining entry to premises.

189. This creates a risk that, once an interception power is authorised under a computer access warrant or data disruption warrant, it could be exercised, without any specific external authorisation or supervision, in a very broad range of circumstances during a warrant operation. For example, a warrant that authorised the interception of telecommunications, without any warrant-specific conditions or limitations being applied to further limit the purposes of interception, would permit an agency to:

- intercept a person's voice or text-based communications for the purpose of determining whether they are, or will be, present at particular premises to which covert entry is sought under the warrant; or
- disable or 'hijack' security systems at those premises which are connected to the internet, such as surveillance cameras or digital authentication points, for the purpose of covertly entering and exiting those premises under the warrant.

Low thresholds for exercising interception powers

190. In addition, the exercise of the telecommunications interception power under a data disruption warrant, and currently under computer access warrants, is not subject to a specific threshold of necessity or proportionality in relation to each interception activity.

191. Rather, when a warrant is issued, it confers a general authority to intercept telecommunications for the purpose of doing any of the acts or things authorised under the warrant. Decisions about whether an interception power should be exercised are entirely at the discretion of the officers executing the warrant.[73] The absence of a specific statutory threshold for the exercise of interception powers under a warrant aggravates the risks outlined above, in relation to overbreadth in the purposes for which interception can be carried out.

Broad powers to make subsequent use and disclosures of intercept information

192. The breadth of the telecommunications interception power must also be considered in combination with the breadth of the power under the TIA Act to make subsequent use and disclosure of interception information obtained under a disruption warrant (or a computer access warrant). A law enforcement agency would be authorised to use and disclose such intercept information for the purpose of activities that, among other things, present a risk to public safety; or are or are likely to be a threat to 'security' as that term is defined in the section 4 of ASIO Act.[74]

193. The definition of 'security' in section 4 of the ASIO Act extends well beyond the ordinary meaning of that word. The statutory definition covers matters including terrorism and other politically motivated violence, foreign interference and espionage, serious threats to Australia's territorial and border integrity, and fulfilling Australia's obligations to other countries in relation to such matters.

194. This means that AFP and ACIC will be able to use intercept information obtained under a data disruption warrant for the investigation of offences that relate to the subject matter covered by the definition of 'security' in the ASIO Act (such as offences with respect to terrorism, foreign incursions, foreign interference and official

[73] Bill, Schedule 1, item 13 (inserting proposed paragraph 27KE(1)(h) of the SDA).

[74] Ibid, item 56 (inserting new section 63AD of the TIA Act). See also the equivalent secondary use, disclosure and dealing provisions for computer access intercept information in existing sections 63AB and 63AC (covering interception information obtained under computer access warrants).

secrecy). It also means that intercept information obtained under a data disruption warrant can be passed to ASIO for the purpose of that organisation performing any of its statutory functions in relation to security. This includes using that interception information as a basis for ASIO obtaining its own intrusive or coercive intelligence collection warrants, and cooperating with other domestic or foreign agencies.

195. The Law Council cautions that, the wider the power to intercept telecommunications under data disruption warrants (and computer access warrants):

- the greater the volume of intercept information that will be collected without any specific authorisation under the TIA Act (and will also bypass the specific reporting and oversight arrangements for interception warrants); and
- the greater the scope for secondary use and disclosure of that intercept information in accordance with the broad permitted disclosure provisions of the TIA Act (as amended by the Bill).

Recommended amendments

Scope of interception power

196. For the above reasons, the Law Council remains concerned about overbreadth in the existing telecommunications interception power under law enforcement and ASIO computer access warrants. These provisions should not be replicated in relation to any of the new warrant types proposed in the Bill.

197. Rather, any power to intercept telecommunications under a computer access warrant, data disruption warrant, network activity warrant or an account takeover warrant should be limited to a subset of specific activities authorised under the warrant. This should cover the specific purpose of gaining access to relevant data, and in the case of disruption warrants, performing a data disruption activity. As a minimum, there should be no power to intercept telecommunications for the purpose of gaining entry to, or exiting, premises under the warrant.

Threshold for exercise

198. The exercise of an interception power should also be subject to a specific threshold of **necessity**, as is presently the case in proposed paragraph 27KE(7)(a) for activities that are likely to cause material interference with, or interruption or obstruction of, the lawful use of computers by non-suspects.

199. However, if the necessity threshold is not supported, then as a minimum, the threshold should be equivalent to that in proposed subparagraph 27KE(2)(e)(i).[75] This would require an assessment that it is reasonable to carry out the interception activity in all of the circumstances, having specific regard to other methods, if any, which are likely to be as effective as interception.

Recommendation 10—scope of telecommunications interception power

- **The telecommunications interception power in proposed subsection 27KE(2)(h) of the SDA (Schedule 1, item 13) should be amended so that it can only be exercised:**

[75] Bill, Schedule 1, item 13. Proposed paragraph 27KE(2)(e) applies the threshold noted above to the actions of the AFP or ACIC (as applicable) in using a computer other than the target computer, or a communication in transit, to access or disrupt the relevant data under the warrant.

- **for the purpose of a sub-set of the activities in proposed subsection 27KE(2) that may be authorised under a disruption warrant. In particular, interception should be limited to accessing data and performing disruption activities. Interception should not be permitted for the purpose of entering or exiting premises under a disruption warrant; and**

- **if it is <u>necessary</u> to intercept a telecommunication for the purpose of doing one or more of those activities.**

- **Equivalent amendments should be made to the computer access warrant provisions in paragraph 27E(2)(h) of the SDA and paragraph 25A(4)(ba) of the ASIO Act.**

Use of force against persons and things

200. Proposed paragraph 27KE(8)(a) provides that all data disruption warrants **must** authorise the use of force against persons and things, where such force is reasonably necessary to do any act or thing authorised under the warrant. In other words, if an issuing authority decides to issue a data disruption warrant, they will have no discretion in the authorisation of force. This is equivalent to existing provisions of the computer access warrant regimes in the SDA and ASIO Act.[76]

Overbreadth in the purposes for which force may be used

201. The Law Council has previously raised concerns about the overbreadth in the purposes for which force can be used, in the context of the TOLA amendments to computer access warrants. The extrinsic materials to the TOLA Bill advanced a case for the use of force in order to enter or exit premises, such as pushing past a person who is obstructing entry or exit points, or to breach open a locked door or cabinet. However, no case was advanced for using force against persons or things to carry out any of the other activities authorised under a computer access warrant.

202. For example, the Law Council considers that there is unlikely to be any credible or rational need for an executing officer to use force against persons or things for the purpose of intercepting telecommunications under a computer access warrant, or a data disruption warrant. However, this is permitted under the current computer access warrant provisions, which are proposed to be replicated in relation to data disruption warrants. The TIA Act does not, and has never, authorised the use of force under interception or stored communications warrants. A similar observation could be made about data disruption activities.

203. The justification advanced by the Department of Home Affairs for the broad scope of telecommunications interception powers under computer access warrants suggested that the power was needed to enable access to premises on which an interception activity is being carried out.[77] However, the Law Council notes that any use of force for the purpose of entering and exiting premises is separate to using force for the purpose of carrying out an interception activity on those premises. It is separately covered by the power to use force for the purpose of entering or exiting any premises, where such entry or exit is necessary to do another act or thing authorised under the warrant (which includes telecommunications interception).

[76] SDA, paragraph 27E(6)(a) and ASIO Act, paragraph 25A(5)(a).

[77] See, for example, Department of Home Affairs, *Supplementary Submission 18.3 to the PJCIS Inquiry into the TOLA Bill*, (November 2018),6 at [19].

204. The Law Council acknowledges that there may be circumstances in which a person executing a warrant may need to carry out an interception activity or a data disruption activity outside a secure facility (for example, in a public place, or in premises that were entered under a warrant). However, if an officer were to be discovered by a target or other person while carrying out that interception or data disruption activity, the general law of self-defence would cover any circumstances in which the use of force may be needed under those circumstances.

205. Any special treatment, by way of conferring a discrete power to use force under a disruption warrant (or presently under a computer access warrant) has not been substantiated. It is no small thing to authorise an agent of the state to use physical force against an individual or private property. This is one of the most intrusive, and potentially harmful, powers that the state can exercise against its citizens and other persons who are physically present within its territorial jurisdiction.

206. Accordingly, if such powers are to be conferred, they must be limited precisely to the circumstances in which a genuine and compelling operational necessity has been established. A generalised appeal to the objective of operational flexibility, or making contingency to address a hypothetical possibility, would not be a sufficient justification. The provisions of the Bill, and existing provisions of the SDA and ASIO Act in relation to computer access warrants, do not meet this standard.

Overbreadth in the persons who may use force under a warrant

207. Additionally, there is overbreadth in the persons who may use force under a data disruption warrant, or a law enforcement computer access warrant under the existing provisions of Division 4 of Part 2 of the SDA.

208. There are no specific provisions under the SDA governing the authorisation of individuals to exercise authority under a warrant, including the use of force. The Bill does not propose to establish such an authorisation regime for the execution of any of the new types of warrants.

209. The absence of specific authorisation requirements for the use of force is particularly problematic in view of public statements suggesting that staff members of ASD are likely to execute at least some of the data disruption warrants issued to the AFP and ACIC.[78] These staff members of ASD would be automatically authorised to use force against persons and things whenever a disruption warrant is issued, for **any activity** that is authorised under the warrant, including data disruption and telecommunications interception. The relevant issuing authority will have no discretion in the matter, other than to decline to issue the warrant in entirety.

210. Further, the provisions of the Bill governing applications for data disruption warrant do not include any requirements for all warrant applications to specify the persons who are proposed to execute the warrant, if issued, and provide details of their training and accreditation to use force, if they are not police officers. The absence of a requirement for all warrants to pro-actively provide this information may limit the ability of issuing authorities to consider the proportionality of the powers that would be conferred under the proposed warrant, with respect to the use of force.

Recommended enhancements to statutory parameters for the use of force

211. The Law Council recommends that the power to use force against persons and things under all of the new warrant types, and existing computer access warrants,

[78] The Hon Peter Dutton MP, Minister for Home Affairs, *Transcript of joint press conference with the Prime Minister*, Parliament House, Canberra, 6 August 2020.

should be subject to stronger statutory parameters in relation to the purposes for which force may be used, and the authorisation of persons to exercise such force.

Recommendation 11—scope of power to use force against persons and things

- **The power to use force against persons or things in proposed paragraph 27KE(8)(a) of the SDA (Schedule 1, item 13) should be amended as follows:**
  - **the issuing authority should have discretion to authorise the use of force under each warrant, as is the case for the other activities specified in proposed subsection 27KE(2);**
  - **the statutory power to use force against persons or things should only be conferred for the purpose of entering or exiting premises, where that is authorised under proposed paragraphs 27KE(2)(a) and (b); and**
  - **the statutory power to use force against persons or things should be limited to particular persons or classes of persons (being police officers, or others who have been specifically trained and accredited in the use of force) and not any person who exercises authority under a warrant.**
- **Equivalent amendments should be made to existing paragraph 27E(6)(a) of the SDA and existing paragraph 25A(5A)(a) of the ASIO Act, which authorise the use of force against persons and things under computer access warrants.**

Temporary removals of computers and other things from premises

212. Proposed paragraph 27KE(2)(f) and subsection 27KE(3) authorise the temporary removal and return of a computer or any other thing from warrant premises, for the purpose of doing any act or thing specified in the warrant under subsection 27KE(2).

213. The Law Council has previously raised concerns about equivalent temporary removal provisions under law enforcement and ASIO computer access warrants in paragraph 27E(2)(f) of the SDA and paragraph 25A(4)(ac) of the ASIO Act, as enacted by the TOLA Act.[79] These issues remain outstanding, and the Bill proposes to extend the provisions of concern to the new warrant-based powers.

214. The Law Council has four key concerns with the temporary removal power, as outlined below. It recommends that these issues are rectified across all existing and proposed warrant regimes, as a prerequisite to the passage of the Bill.

Importance of statutory time limits for removal

215. There is no clear time limit for the temporary removal of a computer or other thing from premises under proposed paragraph 27KE(2)(f).

216. Rather, proposed subsection 27KE(3) requires its return within 'a reasonable period' as determined by the AFP or ACIC in the circumstances. This could be a protracted period, given that data disruption warrants can be in force for up to 180 days in total (comprising 90 days, with the ability to obtain an extension for a further 90 days).

[79] See, for example, Law Council, *Supplementary submission to the PJCIS Review of the TOLA Act*, (August 2020), Attachment 1, 24 (citing previous submissions to the PJCIS Review of the TOLA Bill and the Third INSLM Review of the TOLA Act).

The total period of removal would be solely at the discretion of executing officers, without external authorisation of the precise period.

217. The third INSLM, in his report on the TOLA measures, shared the concern raised by the Law Council about equivalent provisions in the computer access warrant provisions of the SDA and ASIO Act, which do not contain any statutory mechanisms to ensure that a computer or other thing is not removed for a longer period of time than is necessary to do an act or thing under the warrant. The third INSLM recommended amendments to:

> *require that a computer or thing which is removed from warrant premises during the execution of a computer access warrant (or related authorisation) be returned to warrant premises if returning the computer or thing is no longer prejudicial to security or, otherwise,* ***as soon as is it reasonably practicable to do so*** [emphasis added].[80]

218. Rather than correct the issues identified by the third INSLM in relation to computer access warrants, the Bill proposes to repeat these problematic provisions in relation to the new warrant-based powers it seeks to confer.

Need for a clear statutory obligation to return removed items after a warrant expires

219. The Bill does not include any provisions which clearly prescribe the obligations of the AFP or ACIC if a computer or other thing is removed from premises under a data disruption warrant in accordance with paragraph 27KE(2)(f), but has not been returned to those premises when the data disruption warrant ceased to have effect. For example, this could occur because the warrant expires or is revoked.

220. In particular, the following provisions create ambiguity about the applicable obligations of the AFP and ACIC in these circumstances:

- the obligation in proposed subsection 27KE(3) to return a computer or other thing to the premises within a 'reasonable period' appears to apply **only** while a warrant is in force, not after it ceases to be in force;[81]
- it is not clear that the post-warrant concealment power in proposed paragraph 27KE(9)(f) would authorise entry to premises in all instances in which a computer or other thing needs to be returned, because this power is limited to the purpose of concealing that an act or thing was done under a warrant. There may be circumstances in which returning a computer or other thing is not necessary for the purpose of concealing the fact that certain things were done under a warrant. For example, the warrant operation may become known to certain persons who own or lawfully use the computer or other thing that has been removed, and they request its return;
- further, proposed paragraph 27KE(1)(f) does not clearly cover the return only of a computer or other thing that has already been removed under a warrant

[80] Dr James Renwick SC, INSLM, *Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, (30 June 2020), 242-243 at [12.64]-[12.69] and recommendation 15.

[81] This reflects that proposed subsection 27KE(3) does not expressly require a computer or thing to be returned after the warrant ceases to be in force (and confer the necessary power to enter premises to effect its return). Its statutory context appears to support an interpretation that is limited to the time at which the warrant is in force. In particular, proposed subsection 27KE(3) is drafted as a supplement to a set of provisions in subsection 27KE(2), which prescribe the acts or things that can be done while a warrant is in force. Post-warrant activities are dealt with separately in proposed subsection 27KE(9) and are directed exclusively to the purpose of concealing, if necessary, the fact that an act or thing was done under the warrant while it was in force. Subsection 27KE(9) does not clearly **oblige** the AFP or ACIC to return a computer or other thing that is still in their possession at the time the disruption warrant ceases to be in force.

while it was in force. Rather, it appears to cover the compound action of post-warrant 'removal-and-return' of an item, for the purpose of concealing an act or thing previously done under the warrant while it was in force; and

- in any event, proposed paragraph 27KE(1)(f) only confers a discretion to do acts or things after a warrant has ceased to be in effect. This falls short of imposing an obligation on the AFP or ACIC to return a computer or other thing that was removed under the warrant while it was in force, and it had not been returned before the warrant ceased to be in force.

Ambiguity and overbreadth in the meaning of 'other things' that may be removed

221. The meaning of the 'other things' that can be removed from premises, in addition to computers, under proposed paragraph 27KE(2)(f) is unclear. It is not explicitly limited to things that have some connection with a computer, such as data storage devices or other peripheral equipment that can be connected to, or operated in conjunction with, a computer. Nor is it clear that the expression 'other thing' would necessarily be read down in light of the previous word 'computer'.

222. Further, the concept of an 'other thing' has the potential to be extremely broad, because the removal power in proposed paragraph 27KE(2)(f) can be exercised for the purpose of doing **any act or thing** authorised under the warrant, such as entering or exiting premises. It is not limited to the temporary removal of items from premises for the purpose of accessing or disrupting data that is held on, or is accessible from, a computer (for instance, to enable the AFP or ACIC to use more specialised equipment located at a secure facility).

223. For example, there is nothing in proposed section 27KE that would prevent the temporary removal power in proposed paragraph 27KE(2)(f) from authorising an executing officer to remove a set of keys or a smart card from premises covered by the warrant, for the purpose of the AFP or ACIC having copies made to facilitate their access to the premises under proposed paragraphs 27KE(2)(a) and (b) when they are executing the data disruption warrant.

224. This has the potential to be highly intrusive, especially given the breadth of the definition of a 'computer' and the lengthy duration of data disruption warrants. Premises could be accessed on a very large number of occasions while a warrant is in force, to perform multiple acts of data disruption, and multiple post-warrant concealment activities under proposed subsection 27KE(9) after the warrant ceases to be in force. There is also no statutory obligation for any duplicate keys or access cards to be destroyed after a warrant operation ceases, or the post-warrant concealment period ends.

Removal of computers or things may cause material interference or loss

225. As noted above, proposed paragraph 27KE(7)(a) provides that the AFP or ACIC can only do an act or a thing that is likely to cause material interference with, interruption to, or obstruction of a third-party computer user, if causing that impact is **necessary** to do the act or thing. Further, proposed paragraph 27KE(7)(b) provides that the AFP or ACIC can only do an act or thing that causes any other material loss or damage to third-party computer users if justified and proportionate, having regard to the offences covered by the warrant.

226. However, it is unclear how the requirements in proposed subsection 27KE(7) will apply to the actions of the AFP and ACIC in removing computers or other things from premises under proposed paragraph 27KE(2)(f) and subsection 27KE(3).

227. It may be difficult, and potentially impossible, for the AFP or ACIC to accurately ascertain the likely impacts of the temporary removal of a computer or other thing from premises on non-suspects who may use, or otherwise be reliant, upon that computer or thing. In particular, it may be impossible to identify the persons who use, or are otherwise reliant on, the computer or other thing that the AFP or ACIC intends to remove. In this event, the AFP and ACIC are unlikely to be in a position to accurately apply the thresholds in proposed subsection 27KE(7) in relation to the temporary removal power.

228. As a general proposition, the Law Council notes that most people depend heavily on computers to conduct their routine business and personal affairs. On this basis, it could reasonably be inferred that:

- the temporary removal of a computer from premises is likely to cause material interference with the ability of people to lawfully use that computer, or other computers with which it is networked; and
- if a computer is unavailable while it has been temporarily removed from premises, then the people who are reliant on that computer to lawfully conduct their business are likely to suffer financial loss, such as loss of income or expenses to ensure business continuity. A business may also suffer further financial loss arising from reputational damage caused by the outage of their services.

229. For this reason, the Law Council submits that the thresholds of necessity and proportionality in proposed subsection 27KE(7) should apply, as a matter of course, to all temporary removals carried out under proposed paragraph 27KE(2)(f).

Recommendation 12—statutory safeguards on temporary removal power

- **The power to temporarily remove computers and other things from premises in proposed paragraph 27KE(2)(f) and subsection 27KE(3) (item 13 of Schedule 1) should be amended as follows:**
  - **the AFP and ACIC should be subject to an explicit timeframe to return a computer or other thing that is removed from premises. They should be required to obtain a further warrant to retain the computer or other thing for any longer period, including after the warrant ceases to be in force;**
  - **the 'other things' which can be removed from premises should be limited to data storage devices and other peripheral items for the operation of a computer, and only for the purpose of accessing or manipulating data, or performing data disruption activities under paragraphs 27KE(2)(c)-(e) and (g); and**
  - **the removal of a computer or another thing from warrant premises should be subject to an explicit threshold of necessity and proportionality.**

Concealment of things done under a data disruption warrant

230. Proposed subsection 27KE(9) authorises a range of activities that are equivalent to those in proposed subsection 27KE(2) for the purpose of concealing the fact that an act or thing was done under a data disruption warrant.

231. The post-warrant concealment powers in proposed subsection 27KE(9) are exercisable while the data disruption warrant is in force, as well as a period of time

after it has ceased to be in force. This is either 28 days from the day after the warrant ceased to be in force, or the earliest opportunity after that 28-day period.

232. All of the concerns the Law Council has raised above about overbreadth and absence of safeguards in the powers in proposed subsection 27KE(2) apply equally to the post-warrant concealment powers in proposed subsection 27KE(9).

233. In addition, the Law Council is concerned about the lengthy and potentially indeterminate amount of time for which post-warrant concealment powers could be exercised. This is particularly because the task of concealing the 'digital footprint' of computer-related activities may have very different requirements to the 'one-off' actions that may be required to conceal physical access to premises. That is, the task of concealing previous access to, or modification or disruption of, data held in a computer may require repetitive actions over an ongoing period of time to conceal, and thereafter continue to conceal, the relevant cyber-enabled activities.

234. These factors led the third INSLM to recommend that the identical provisions governing post-warrant concealment for computer access warrants under the subsection 27E(7) of the SDA and subsection 25A(8) of the ASIO Act should be amended to require the relevant agency to:

> *seek external authorisation to exercise a concealment of access power if it proposes to take that step more than 28 days after the warrant has expired.*[82]

235. The Bill proposes to confer post-warrant concealment powers for data disruption warrants in contradiction of the design principles recommended by the third INSLM.

Recommendation 13—statutory safeguards for post-warrant concealment powers

- **The powers of post-warrant concealment in proposed subsection 27KE(9) should be amended as follows:**
  - **the matters in the Law Council's recommendations 8-12 in relation to proposed subsection 27KE(2) should be applied equally to the corresponding concealment powers in proposed subsection 27KE(9); and**
  - **the power to undertake a post-warrant concealment activity more than 28 days after the warrant has expired should require separate, external authorisation by an issuing authority, consistent with the recommendations of the third INSLM in relation to computer access warrants.**
- **The corresponding post-warrant concealment powers for computer access warrants in subsection 27E(7) of the SDA and subsection 25A(8) of the ASIO Act should also be amended accordingly.**

Duration of data disruption warrants

236. Proposed subsection 27KD(2) provides that a data disruption warrant may only be issued for a period of 90 days (three months). Proposed paragraph 27KF(1)(a) provides that the issuing authority may, upon further application by the AFP or ACIC,

[82] Dr James Renwick SC, INSLM, *Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, (30 June 2020), 240-241 at [12.56]-[12.63] and recommendation 14.

extend a data disruption warrant for up to a further 90 days. This would bring the total period of effect for a data disruption warrant to 180 days (six months).

237. The Law Council acknowledges that this maximum period of effect is aligned with the maximum duration of surveillance device warrants and computer access warrants under the existing provisions of the SDA.[83] However, such alignment overlooks fundamental differences in the nature of data disruption powers (to frustrate the commission of an offence by means other than enforcement), and digital surveillance powers (for the purpose of collecting admissible evidence to support arrest, charge and prosecution).

238. The Law Council considers that data disruption warrants should be subject to a shorter maximum duration of 90 days (inclusive of any extensions, if a warrant is initially issued for a period of less than 90 days).

239. The ability to obtain a data disruption warrant for a total duration of 180 days, with no limit on the number of consecutive warrants that may be issued, creates a real risk that data disruption could lawfully be used as a *de facto* substitute for the enforcement of offences. In other words, the Bill as presently drafted would make it lawful for enforcement agencies to elect to engage in data disruption activities in perpetuity, in preference to enforcing offences, despite the availability of sufficient, admissible evidence to support prosecutions. This reinforces the caution raised by the Richardson Review, noted above, that the conferral of data disruption powers on law enforcement agencies could effectively make them the 'judge, jury and executioner' in relation to cyber-enabled offences.

240. The Law Council considers it essential that the fundamental difference between the purpose of data disruption warrants on the one hand, and existing computer access warrants and surveillance device warrants on the other hand, is reflected in a comparatively shorter maximum duration for data disruption warrants.

241. If the AFP or ACIC consider that there is a need to engage in data disruption over a longer period of time than 90 days (including extensions), they should be required to seek authorisation under a fresh warrant. This would ensure that there is an assessment *de novo* (anew) of the entire basis for the issuance of the warrant. This includes each of the discretionary activities authorised under proposed subsection 27KE(2), and any warrant-specific conditions applied to those activities.

242. This would also ensure that, if data disruption powers are available to the AFP or ACIC for a prolonged period of time under consecutive disruption warrants, these agencies would need to prepare a warrant report for each individual warrant. The effect is that reports on the warrant operation would need to be provided to the Minister approximately every three months. Otherwise, if the total maximum period of effect were to remain at 180 days, warrant reports would only need to be provided every six months. The Law Council submits that six months is a disproportionately long reporting interval, given the novel and highly intrusive nature of data disruption powers, including the ability to cause material loss or damage to third parties who are lawfully using a computer.

Recommendation 14—limitations on extensions of data disruption warrants

- **Proposed subsections 27KD(2) and 27KF(1) (item 13 of Schedule 1) should be amended to provide that the total maximum duration of a**

[83] SDA, sections 19 and 27F.

data disruption warrant is 90 days, inclusive of any extensions if the warrant is initially issued for a period of less than 90 days.

- **If the AFP or ACIC consider that there is a need to carry out further data disruption activities after the 90-day total maximum period of effect for a data disruption warrant, then they should be required to seek a new warrant.**

Extraterritoriality

243. Proposed section 43C of the SDA contains provisions enabling the extraterritorial execution of data disruption warrants, which are similar to existing provisions of the SDA in relation to surveillance device warrants and computer access warrants.[84]

244. In short, offshore data disruption activities will only be permitted if a relevant official of the foreign country has consented to the activity being carried out in the foreign country.[85] However, the consent requirement will not apply if the persons executing the data disruption warrant are physically present in Australia, and the geographical location of the relevant data is unknown, or cannot reasonably be determined.[86]

Overlap with ASD's functions to prevent and disrupt cybercrime outside Australia

245. The Law Council is concerned that any extraterritorial application of data disruption warrants will overlap with or duplicate the existing functions of ASD under paragraph 7(1)(c) of the ISA, with respect to the disruption and prevention of cybercrime undertaken by persons or organisations outside Australia, via electronic or other similar means.

246. The Bill appears to replicate existing provisions of the SDA governing the extraterritorial application of surveillance device warrants and computer access warrants,[87] without acknowledging the specific and novel context of data disruption as a form of 'offensive' cyber security action, or justifying the perceived need for extraterritorial application in this context.

247. The Explanatory Memorandum does not acknowledge, or offer justification for, the resultant overlap with the functions of ASD under paragraph 7(1)(c) of the ISA. It simply states that there is an intention for data disruption warrants to be subject to the same principle of consent-based extraterritoriality that currently apply to surveillance device warrants and computer access warrants under the SDA.[88]

248. Proposed section 43C of the SDA also appears inconsistent with the position evident in the unclassified report of the Richardson Review, that ASD should be the sole agency responsible for undertaking 'offensive' cyber activities outside Australia to prevent and disrupt cybercrime, under its existing statutory functions in the ISA. This was reflected in the Review's recommendations and findings to the effect that:

    - ASD's disruptive and preventive functions in relation to cyber-enabled crime should remain limited to the activities of people and organisations located outside Australia, including Australian persons where a ministerial authorisation has been issued under the ISA;

[84] SDA, Part 5, especially sections 42 and 43A.
[85] Bill, Schedule 1, item 27 (inserting proposed subsections 43C(1)-(3) of the SDA).
[86] Ibid (inserting proposed subsection 43C(4) of the SDA).
[87] SDA, sections 42 and 43A.
[88] Explanatory Memorandum, 47 at [182].

- there is a valuable role for the National Intelligence Community in disrupting cyber-enabled offending 'onshore' (inside Australia) through means other than prosecution, and 'this role rightly sits with the AFP', not ASD; but
- the AFP (and, by extension, any other law enforcement agencies that also perform disruption activities, such as the ACIC) did not require specific statutory powers to engage in 'onshore' disruption activities via electronic means, to prevent or disrupt cyber-enabled crime.[89]

249. The Law Council is concerned that the duplication created by proposed section 43C of the SDA creates a risk of conflict or inconsistency in the offshore disruption activities undertaken by ASD, the AFP and ACIC, including as a result of significant differences in applicable authorisation thresholds and processes and oversight mechanisms.

250. Any duplication of powers to disrupt cyber-enabled crime by persons or organisations outside Australia could also jeopardise the security and effectiveness of offshore disruption operations (for example, if de-confliction and coordination mechanisms are inadequate or ineffective). It may also lead to inefficiencies in the use of public resources by multiple agencies in conducting substantially similar disruption operations outside Australia.

251. As the extrinsic materials to the Bill do not contain any justification of the need for data disruption warrants to have extraterritorial application, on top of the existing functions of ASD under paragraph 7(1)(c) of the ISA, the Law Council recommends that proposed section 43C of the SDA is removed from the Bill.

Recommendation 15— no extraterritorial application of data disruption warrants

- **The Bill should be amended to omit proposed section 43C of the SDA (Schedule 1, item 27).**
- **Rather than data disruption warrants having extraterritorial application, ASD should have exclusive responsibility for undertaking activities outside Australia to prevent and disrupt cyber-enabled crime, pursuant to paragraph 7(1)(c) of the ISA.**

Emergency authorisations

252. Items 15-24 of Schedule 1 to the Bill propose to extend the existing emergency authorisation provisions of Part 3 of the SDA to data disruption warrants. Currently, those provisions cover surveillance device and computer access powers.

253. The emergency authorisation regime in Part 3 enables any 'law enforcement officer' to apply to an 'appropriate authorising officer'[90] within their agency for an emergency authorisation. This is only available in defined circumstances of emergency, where there is a need for immediate action, and it is not practicable to apply for a warrant.[91]

254. If an internal authorisation is granted, an application must be made to an issuing authority within 48 hours for a retrospective approval of the emergency authorisation. A concurrent application may also be made for a warrant to

[89] Richardson Review, *Unclassified Report,* Volume 3, (December 2019), recommendations 161 and 162. See also the discussion at pp. 218-219 at [38.58]-[38.65].

[90] SDA, subsection 6A(4). For the AFP, this is the Commissioner, Deputy Commissioner or an SES employee who is authorised by the Commissioner (table item 5, column 4). For the ACIC, this is the CEO or an executive level staff member authorised by the CEO (table item 15, column 4).

[91] SDA, subsections 28(1) and (1A). See also, Bill, Schedule 1, item 15 (inserting new subsection 28(1C).

prospectively authorise any further surveillance.[92] If the emergency authorisation is not approved retrospectively, the issuing authority may make directions in relation to subsequent dealings with information obtained under the emergency authorisation, but may not order it to be destroyed.[93]

255. The Bill proposes to expand this regime to enable internal authorisation of data disruption activities, but only in relation to one of the defined emergencies in existing Part 3 of the SDA. This is the circumstance prescribed in existing section 28, which covers an imminent risk of serious violence to a person, or substantial damage to property. Under the amendments, the authorising officer would have to be satisfied of the following matters to issue an emergency authorisation for data disruption:

- the disruption of data is immediately necessary for the purpose of dealing with the imminent risk of serious violence or serious property damage;
- the circumstances are so serious, and the matter is of such urgency, that data disruption is warranted; and
- it is not practicable in the circumstances to apply for a disruption warrant.[94]

Appropriateness of emergency authorisations for data disruption powers

256. The Law Council considers that there is a threshold issue as to whether data disruption powers should be subject to a regime of internal authorisation, given that:

- data disruption is a materially different power to conducting electronic surveillance for investigatory purposes; and
- data disruption has the potential to cause much greater harm to non-suspects than surveillance alone.

257. The Explanatory Memorandum restates the legal effect of the proposed emergency authorisation provisions, and does not provide substantive justification for the proposal to expand the existing emergency authorisation regime for surveillance device and computer access warrants to also include data disruption warrants.[95] Nor does the Explanatory Memorandum explain why arrangements for the urgent issuance of warrants, such as remote or oral applications, could not provide sufficient coverage in circumstances of emergency.

258. The proposed amendments to Part 3 of the SDA are not merely a technical or routine exercise in applying existing authorisation mechanisms in the SDA to a similar power to those already authorised by that Act. Rather, they propose to confer a new power of a fundamentally different kind to the existing surveillance powers, which also carries a much higher risk of causing material loss or damage to people who lawfully use or are reliant on computers, and are not under any suspicion of wrongdoing.

259. The Law Council cautions against making an assumption that the existing framework for the authorisation of surveillance powers is automatically suitable for the authorisation of the new data disruption powers. Rather, in the absence of supporting justification in the extrinsic materials to the Bill, data disruption powers should not be subject to the emergency authorisation regime in Part 3 of the SDA.

[92] SDA, sections 33, 34, 35 and 35A. See also, Bill, Schedule 1, item 23 (inserting new section 35B).
[93] Ibid.
[94] Bill, Schedule 1, item 15 (inserting proposed subsection 28(1C) of the SDA).
[95] Explanatory Memorandum, 42-46 at [151]-[174].

260. The Law Council considers that, before any proposal is entertained to expand the emergency internal authorisation regime in Part 3 to data disruption powers, consideration should first be given to legislative and practical measures to facilitate the urgent making and determination of warrant applications.

Recommendation 16—no emergency authorisations for data disruption powers

- **The Bill should be amended to omit the proposed amendments to Part 3 of the SDA (items 15-24 of Schedule 1). Data disruption powers should not be subject to the regime of emergency authorisations.**
- **If there is a need for the expedited approval of data disruption powers in time critical circumstances, then it should be addressed through practical mechanisms to enable the making and determination of warrant applications in urgent cases.**
- **Consideration could be given to legislative amendments to create a discrete regime for requesting and issuing emergency warrants. However, this course should be taken only if it is established that the general provisions governing warrant applications and issuing decisions would not operate effectively in urgent cases.**

Thresholds for emergency authorisations

261. If the Law Council's primary recommendation for the removal of emergency authorisation powers from the Bill is not implemented, then the Law Council alternatively recommends that the threshold for the internal authorisation of data disruption powers in proposed subsection 28(1C) should be strengthened.

'Last resort' requirement

262. The Law Council recommends that the criterion in proposed paragraph 28(1C)(c), requiring satisfaction that data disruption is warranted in view of the severity and urgency of the circumstances, should be replaced with a 'last resort requirement'.

263. That is, the authorising officer must be satisfied that there are no other alternatives which are likely to be as effective in avoiding the imminent risk of serious violence or substantial property damage that the applicant has identified. (Examples of alternatives would include exercising powers of arrest and charge in relation to an offence.) This would ensure that the power to internally authorise data disruption is limited to those circumstances in which it is strictly necessary, in that there are no other viable alternatives to an internal authorisation.

264. The Law Council emphasises that a last resort threshold would require an assessment of the viability and likely effectiveness of alternatives in the circumstances of each case, and the exclusion of those alternatives if they are not likely to be equally effective. That assessment would take into account the circumstances of urgency and emergency which have prompted the application. Accordingly, it would not necessarily require alternative forms of intervention to have been attempted and failed. In other words, a last resort threshold is capable of operating effectively in circumstances of significant urgency.

265. Strengthening the authorisation threshold in this way would reflect the extraordinary nature of data disruption, as well as the fact that it would be permissible to cause material loss or damage to third parties who use or are reliant on a computer, where this is assessed as being justified. In contrast, emergency authorisations under

existing Part 3 of the SDA for the use of surveillance devices and computer access are subject to an absolute prohibition on causing loss or damage to non-suspects.

Consideration of potential impacts on third parties

266. The Law Council further recommends that the authorising officer must be required to specifically consider the potential impacts on third parties who are not suspects. The authorising officer should only be empowered to issue an emergency authorisation for data disruption activities if satisfied, on reasonable grounds, that the likely impacts of data disruption activities are proportionate to the imminent harm to persons, or damage to property that is sought to be prevented.

267. A statutory condition of this kind would provide the strongest possible assurance that the potential impacts on non-suspects will be given routine and consistent consideration in all applications for emergency authorisations. This should not merely be left to the discretion of individual authorising officers when considering applications. Nor should it be dealt with only in internal operating policies of the AFP or ACIC. Rather, a statutory condition would ensure that there is a legal rule mandating the assessment of this matter in each and every request for an emergency authorisation. Setting this rule in primary legislation will ensure that its establishment and continued existence is not subject to unilateral, and potentially unannounced, repeal or modification by the executive government.

Recommendation 17—last resort threshold for emergency authorisations

- **If emergency authorisations are to be available for data disruption, contrary to the Law Council's primary recommendation above, then proposed section 28(1C) of the SDA (item 15 of Schedule 1) should be amended as follows**:
  - **proposed paragraph 28(1C)(c) should be replaced with a requirement for the authorising officer to be satisfied, on reasonable grounds, that there are no alternative means available to prevent or minimise the causation of serious violence or substantial property damage that are likely to be as effective as data disruption, in the particular factual circumstances; and**
  - **the authorising officer should also be required to consider the likely impacts of the proposed data disruption activity on third parties who are using, or are reliant on, the target computer. The authorising officer should only be able to grant the emergency authorisation if satisfied, on reasonable grounds, that:**
    - **adequate arrangements are in place to minimise, to the greatest possible extent, those impacts; and**
    - **any likely impacts on third parties are proportionate to the objective of the emergency authorisation, to prevent or mitigate serious, imminent violence or property damage**.

Obligations if issuing authority does not retrospectively approve an authorisation

268. If there is an appetite for an emergency authorisation regime to apply to data disruption powers, the Law Council further recommends that issuing authorities should be conferred with stronger powers to issue directions in relation to acts done, or information obtained, under emergency data disruption authorisations. These powers should be tailored specifically to the nature of data disruption activities, as distinct to existing surveillance powers for investigatory purposes.

269. Proposed subsections 35B(3) and (4) of the SDA (item 23 of Schedule 1 to the Bill) simply replicate the existing powers available to issuing authorities under Part 3 of the SDA, if they decline to retrospectively approve an emergency authorisation for the use of a surveillance device or computer access. They enable the issuing authority to direct that the relevant activities cease, and to make such orders as they consider appropriate about the manner in which information obtained under the emergency authorisation (or records or that information) must be dealt with. However, this expressly excludes the power to order the destruction of information obtained under warrants, or records that are related to that information.[96]

270. The Law Council considers that more tailored powers are needed to successfully remediate the harmful impacts of internally authorised data disruption activities, which are independently assessed on a retrospective basis as having been issued incorrectly or inappropriately. In particular, the Law Council supports the conferral of powers on the issuing authority to make orders requiring the AFP or ACIC to:

- disclose the existence of a data disruption activity to an owner or operator or user of a computer or data, who has been adversely affected by the data disruption activity (provided that this is not likely to cause serious prejudice to law enforcement operations or capabilities, or Australia's national security); or
- take remedial action, such as the payment of compensation to non-suspects who have suffered loss or damage, the restoration of data that has been manipulated for the purpose of gaining access to other data or carrying out the disruption activity, and the return of items removed from premises.

271. These remedial actions are unique to the purpose and impacts of data disruption powers, in frustrating the commission of an offence by means other than prosecution. They are analogous to the powers of the Investigatory Powers Commissioner under the *Investigatory Powers Act 2016* (UK) (**IPA**). Specifically, the Investigatory Powers Commissioner can require a UK intelligence or law enforcement agency to notify persons who are adversely affected by a serious 'relevant error' by that agency (that is, a failure to comply with applicable legal requirements governing the exercise of investigatory powers) where it is in the public interest to do so. This is subject to exceptions for disclosures that are likely to cause prejudice to security, operational and other national interests.[97]

272. The Commissioner's power to direct an agency to disclose a 'relevant error' enables any person who has been adversely affected to pursue a remedy in the Investigatory Powers Tribunal. Importantly, this notification regime applies to any 'relevant errors' made by GCHQ in the exercise, or purported exercise, of its equipment interference powers.

Recommendation 18—orders if an emergency authorisation is not approved

- **If emergency authorisations are to be available for data disruption, contrary to the Law Council's primary recommendation above, then proposed section 35B (item 23 of Schedule 1) should be amended to confer the following powers on an issuing authority, if they decline to retrospectively approve an emergency data disruption authorisation:**
  - **the issuing authority may require the AFP or ACIC to disclose the existence of the data disruption activity to an owner, operator or user of a computer or data, who has been adversely affected by**

[96] Bill, Schedule 1, item 23 (inserting proposed section 35B of the SDA). See also: SDA, subsections 35(5) and (6) (surveillance device authorisations) and subsections 35A(5) and (6) (computer access authorisations).
[97] *Investigatory Powers Act 2016* (UK), section 231.

the disruption activity. This should be subject to a requirement to be satisfied that such disclosure is not likely to cause serious prejudice to law enforcement operations or capabilities or national security; and

- **the issuing authority may require the AFP or ACIC to take such remedial action as considered appropriate in the circumstances, including, but not limited to, financial compensation.**

'Appropriate authorising officers' for emergency data disruption powers

273. The Bill proposes to confer emergency authorisation functions for data disruption powers on 'appropriate authorising officers' of the AFP and ACIC, as defined in existing section 6A of the SDA.

274. The Law Council is satisfied that the 'appropriate authorising officers' for the AFP are persons of a sufficient level of seniority, being the AFP Commissioner, a Deputy Commissioner or a Senior Executive Service-level employee who has been appointed by the AFP Commissioner.[98]

275. However, for the ACIC, the CEO may appoint any Executive Level staff member as an 'appropriate authorising officer'.[99] While any such person must be specifically approved by the CEO, the Law Council is concerned that persons of a 'mid-management' classification, who could potentially be provided on secondment from other agencies, do not possess a level of seniority that is commensurate with the extraordinary nature of data disruption, especially in the circumstances of emergency in which emergency authorisations would be issued.

276. The Law Council recommends that the Bill should be amended to provide that the persons who may issue emergency data disruption authorisations to the ACIC are the CEO of that agency, and any Senior Executive Service-level employee who has been appointed by the CEO to issue these emergency authorisations.

Recommendation 19—'appropriate authorising officers' for the ACIC

- **If emergency authorisations are to be available for data disruption, contrary to the Law Council's primary recommendation above, then the Bill should be amended to provide that the following persons are authorised to issue emergency data disruption warrants for the ACIC:**
  - **the CEO of the ACIC; and**
  - **a Senior Executive Service-level employee of the ACIC, who has been authorised in writing by the CEO to issue emergency authorisations for data disruption.**

Oversight and reporting

277. The existing functions and powers of inspection conferred on the Commonwealth Ombudsman under Division 3 of Part 6 of the SDA will apply to data disruption warrants and emergency authorisations.

278. This will enable the Ombudsman to conduct six monthly inspections of all data disruption warrants and emergency authorisations, for the purpose of assessing

[98] SDA, subsection 6A(4) and table item 5, column 4.

[99] Ibid, table item 15, column 4.

compliance with the requirements of the SDA, and reporting to the Minister for Home Affairs (who is required to table those reports in Parliament within 15 sitting days of receipt).[100]

279. The Ombudsman would also have functions under the *Ombudsman Act 1976* (Cth) (**Ombudsman Act**) to investigate complaints in relation to matters of administration arising from the execution of a data disruption warrant by the AFP or ACIC.

280. In addition, proposed section 49C of the SDA requires the AFP and ACIC to notify the Ombudsman when a warrant is issued and an act is done under a warrant, within seven days of doing the act.[101]

281. Subject to the matters of detail discussed below, the Law Council welcomes the inclusion of provisions in the Bill which are intended to support the independent operational oversight of the data disruption regime. This includes notification requirements, to help focus oversight on high-risk and intrusive activities.

282. However, the Law Council also emphasises that a bi-annual, retrospective inspection function, while valuable, is no substitute for its earlier recommendations to improve the independence and rigour in the issuing process for data disruption warrants. That includes by designating issuing authorities as superior court judges alone; strengthening issuing thresholds; and incorporating greater precision in the scope of the powers able to be authorised under data disruption warrants.

Absence of notification requirement for post-warrant concealment activities

283. Existing section 49B of the SDA requires a law enforcement agency to specifically notify the Ombudsman if the agency undertakes any post-warrant concealment activities in relation to a computer access warrant, where those activities are carried out after the warrant has ceased to be in force, for the purpose of concealing the fact that an act or thing was done under a computer access warrant.

284. In particular, the notification requirement in existing section 49B applies if the concealment-related act was done more than 28 days after the expiry of the computer access warrant. This stand-alone notification requirement ensures that the Ombudsman is informed of post-warrant concealment activities that are not captured by the substantive report on the warrant required under existing subsection 49(2B) because they occur after that report has been finalised. (The warrant reports under existing subsection 49(2B) must be prepared and given to the Minister as soon as practicable after the warrant ceases to be in force, and are accessible to the Ombudsman as part of their inspection function.)

285. In contrast to the existing arrangements for computer access warrants, the Ombudsman notification requirement for data disruption activities in proposed section 49C of the SDA is limited expressly to activities that are carried out **while the warrant is in force** under proposed subsection 27KE(2). It therefore contains two notable omissions:

- concealment activities carried out under proposed subsection 27KE(9) while a disruption warrant is in force, or within 28 days of its cessation (which could be a protracted period, given that the total maximum duration of a data disruption warrant is 180 days, inclusive of an extension of up to 90 days); and
- concealment activities carried out later than 28 days after the warrant ceases to be in force, which could similarly be carried out over a protracted period of

[100] Ibid, sections 55 and 61. See also the Ombudsman's powers of access in sections 56 and 57.

[101] Bill, Schedule 1, item 41 (inserting proposed section 49C of the SDA).

time. (This is especially the case for activities which are carried out to conceal a digital footprint created by a data access or data disruption activity, which may require repeated acts of concealment over an indefinite period.)

286. The post-warrant concealment activities authorised under proposed section 27KE(9) are identical to those able to be authorised under proposed subsection 27KE(2). The only difference is the purpose to which those activities are directed (being concealment of the fact that acts or things were done under a data disruption warrant, rather than accessing and disrupting data under that warrant). Accordingly, there is an equal need to inform the Ombudsman about the exercise of these extraordinary, intrusive powers for the purpose of frustrating the commission of an offence and for the purpose of concealing that such acts were carried out.

287. The Explanatory Memorandum does not explain why proposed section 49C excludes concealment-related acts done under proposed subsection 27KE(9). Nor does it explain why the data disruption warrant regime does not include an Ombudsman notification requirement equivalent to that in existing section 49B of the SDA for post-warrant concealment activities. This is anomalous given that the Bill proposes that data disruption warrants would be capable of authorising all of the acts and things that can presently be done under a computer access warrant, as well as data disruption activities.

Recommendation 20—enhancements to statutory notification requirements

- **The requirements to notify the Ombudsman of certain acts or things done under data disruption warrants should be amended as follows:**
  - **the notification requirement in proposed section 49C (item 41 of Schedule 1 to the Bill) should be expanded to cover concealment-related actions carried out under proposed subsection 27KE(9) while a data disruption warrant is in force, and up to 28 days after it expires; and**
  - **a new provision should be inserted in Division 2 of Part 6 of the SDA, equivalent to existing section 49B in relation to computer access warrants. It should require the AFP and ACIC to notify the Ombudsman of any post-warrant concealment acts carried out under proposed subsection 27KE(9) more than 28 days after a warrant has ceased to be in force.**

Resourcing for independent operational oversight

288. In addition, the Law Council emphasises the importance of the Ombudsman having adequate resources to perform the expanded inspection functions for data disruption warrants, as well as the proposed regime of account takeover warrants in Schedule 3 to the Bill. This resourcing must ensure that the Ombudsman can:

- employ adequate numbers of qualified and security cleared staff;
- have access to personnel, physical and information security measures and infrastructure which enable them and their staff to routinely access information of the highest level of classification that is created or utilised in the relevant warrant operations subject to oversight; and
- have full access to technical expertise relevant to data disruption and account takeover activities, from eminent experts who are wholly independent (both in substance and perception) from the agencies subject to oversight.

Recommendation 21—resourcing for oversight of the new warrant regimes

- **The Government should increase the budget of the Commonwealth Ombudsman, to enable the effective oversight of the new powers conferred by the Bill, including data disruption. Additional resourcing should enable the Ombudsman to:**
  - **have an appropriate number of security-cleared staff to perform inspection, investigatory and complaints handling functions;**
  - **have appropriate security infrastructure, including accredited premises and ICT systems for information of the highest national security classification that is likely to be generated under all of the new warrant regimes proposed in the Bill; and**
  - **access independent technical expertise, to enable effective oversight of the proposed powers, and existing electronic surveillance powers within the Ombudsman's remit.**

A broader inspection remit for the Ombudsman

289. Further, the Law Council questions whether the Ombudsman's inspection function should be expanded beyond a strict assessment of an agency's compliance with the requirements of the SDA, to include broader matters of propriety, compatibility with human rights and a specific mandate to assess compliance with internal policies.

290. This would be consistent with the inspection functions of the IGIS, as set out under the IGIS Act, in relation to the intelligence agencies within its remit.[102] Importantly, the conferral of an equivalent inspection function on the Ombudsman would enable the Ombudsman to conduct, at its discretion, more qualitative reviews of the analytical integrity in decision-making by officers of the AFP and ACIC in determining the necessity and proportionality of requests for disruption warrants or authorisations, and in making decisions about the execution of the broad, discretionary powers conferred by those warrants or emergency authorisations.

291. The Law Council considers that alignment in the scope and focus of the respective inspection functions of the IGIS and Ombudsman is appropriate, having regard to the increasing interoperability between law enforcement and intelligence agencies.

292. Moreover, the Intelligence Oversight and Other Legislation (Integrity Measures) Bill 2020 (separately under review by the Committee) proposes to expand the oversight functions of the IGIS to cover the 'intelligence functions' of the ACIC. This makes it even more important for there to be a consistent approach to the oversight of the ACIC. Additionally, the present Bill proposes to expand the functions of the IGIS to cover the AFP's activities in relation to network activity warrants.[103] This similarly makes it important for there to be a consistent approach to the oversight of all of the AFP's new warrant-based powers in relation to cyber-enabled crime.

[102] IGIS Act, section 8 (intelligence agency inquiry functions of the IGIS).

[103] Bill, Schedule 2, items 55 and 56 (inserting amendments to subsection 3(1) of the IGIS Act to introduce the definition of an 'intelligence function of the AFP'. This covers the collection, correlation, analysis, production and dissemination of intelligence obtained from a network activity warrant, and the exercise of functions or powers by AFP members in relation to the network activity warrant provisions of the SDA. See also new subsection 8(3A) of the IGIS Act, which proposes to confer oversight functions on the IGIS in relation to the 'intelligence functions' of the AFP).

Recommendation 22—expansion of Ombudsman's inspection functions

- **The Ombudsman's inspection functions in relation to the new powers proposed in the Bill, including data disruption, should be expanded to cover matters additional to agencies' compliance with the SDA.**
- **The expanded inspection functions in relation to the AFP and ACIC should be akin to the broader oversight remit of the IGIS in relation to intelligence agencies, under section 8 of the IGIS Act.**

  In particular, it should cover:

  - **agencies' compliance with applicable policies and procedures (as well as the provisions of the SDA and related legislation);**
  - **the propriety of agencies' actions, practices and policies under the new warrant-based regimes; and**
  - **the compatibility of agencies' actions, practices and policies under the new warrant-based regimes with Australia's international human rights obligations.**

Attorney-General's power to restrict the Ombudsman's access to information

293. Existing subsection 9(3) of the Ombudsman Act confers power on the Attorney-General to prevent the Ombudsman from accessing certain information in the course of performing independent oversight functions. It provides that the Attorney-General may furnish a certificate to the Ombudsman, which stipulates that the Ombudsman cannot request or compel the production of specified information, because the Attorney-General has determined that it would be contrary to the public interest for that information to be disclosed to the Ombudsman. Subsection 9(3) of the Ombudsman Act lists various public interest grounds on which information may be withheld at the discretion of the Attorney-General, including the interests of Australia's national security.

294. It is readily conceivable that the covert activities of the AFP or ACIC in disrupting data for the purpose of frustrating the commission of an offence will, by their very nature, involve the creation and use of highly classified information. Consequently, there is the potential for the certification power in subsection 9(3) of the Ombudsman Act to have a wide application to the proposed data disruption regime, at the discretion of the Attorney-General.

295. As was evident in a recent decision of the AAT under the *Freedom of Information Act 1982* (Cth), concerning access to information that the Attorney-General redacted from a report of the Auditor-General prior to its public dissemination, there may be scope for a considerable divergence of views between the Attorney-General and an independent trier of fact on the question of whether withholding certain information would be prejudicial to Australia's national security.[104]

296. For these reasons, the Law Council considers that the Attorney-General's certification power in existing subsection 9(3) of the Ombudsman Act is not appropriate in relation to the Ombudsman's oversight functions over the new data disruption regime in Schedule 1 to the Bill, or the proposed account takeover powers in Schedule 3. The potential for the certification power to apply to most, if not all, information that is generated or utilised by these regimes raises an unacceptable risk that the power could be exercised in a manner which interferes with the

[104] *Patrick and Secretary, Department of Prime Minister and Cabinet* [2020] AATA 4964 (9 December 2020, Britten DP) at [63]-[65].

independence of the Ombudsman in determining whether to investigate a matter, and the focus and manner of conduct of any such investigation.

297. The Law Council submits that subsection 9(3) of the Ombudsman Act should be amended to exclude the new powers proposed in the Bill from the Attorney-General's certification power to withhold information from the Ombudsman. Rather than empowering a Minister the power to restrict the Ombudsman's access to information on national security grounds, it would be preferable for the Government to invest in the organisational capabilities of the Office of the Ombudsman to handle highly classified information, as is the case with the IGIS. (See also recommendation 21 in relation to resourcing of oversight agencies).

Recommendation 23—removal of Attorney-General's certification power

- **The Ombudsman Act should be amended so that the Attorney-General's certification power in subsection 9(3) cannot be invoked to prevent the provision of information to the Ombudsman for the purpose of performing any oversight function in relation to data disruption warrants or emergency authorisations for data disruption.**

Oversight of ASD's actions under data disruption warrants

Variable nature of oversight mechanisms

298. If ASD provides its services to the AFP and ACIC to execute data disruption warrants, as appears to be contemplated at least in some instances, then the applicable oversight arrangements in relation to ASD staff members will depend on the precise legal mechanism by which that assistance is provided.

299. This may vary across different warrant operations, depending on the nature and scale of assistance required from ASD. However, two legal options are open:

- **secondment:** ASD staff members may be seconded to the AFP or ACIC to perform functions for and on behalf of those agencies, as 'law enforcement officers' under the SDA. In this event, the Commonwealth Ombudsman would be responsible for overseeing those staff members' actions in executing data disruption warrants as secondees to the AFP or ACIC; or

- **ASD's cooperation function under the ISA:** ASD staff members could provide assistance to the AFP or ACIC as part of performing ASD's own statutory function in paragraph 7(1)(f) of the ISA to cooperate with other Commonwealth agencies. This is provided that those other agencies are prescribed in regulations made under section 13A of the ISA. This would require regulations to be made listing the AFP and ACIC as agencies with which ASD may cooperate. In this event, ASD staff members would remain subject to the oversight remit of the IGIS, not the Commonwealth Ombudsman, when executing data disruption warrants.[105]

300. The extrinsic materials to the Bill do not provide an indication of the intended legal basis upon which ASD staff members will assist the AFP or ACIC in executing data disruption warrants. Consequently, they do not provide any insight into the

[105] See: IGIS Act, section 3 (definition of a member of an agency) and subsection 3(3) (an agency member's actions are taken to be those of the agency if they do so in their capacity as a member of that agency).

anticipated division of oversight responsibilities between the Ombudsman and IGIS, in relation to ASD staff members who are assisting the AFP or ACIC.

Implications for the nature and scope of oversight functions

301. As noted above, there are differences in the nature and scope of the respective oversight functions and powers of the IGIS and Ombudsman. The Ombudsman is also subject to the exercise by the Attorney-General of powers to prevent access to certain information, whereas the IGIS is not.

302. Unless greater legislative efforts are made to establish consistent oversight arrangements, ASD staff members who are seconded to the AFP or ACIC to execute data disruption warrants may be subject to more limited oversight than would have applied if they were performing the cooperation functions of ASD.

303. For example, there would be no explicit mandate for the inspections of the AFP and ACIC conducted by the Ombudsman to cover matters of propriety, human rights compatibility and compliance with policy and procedure, as well assessing compliance with the applicable provisions of the SDA. However, the IGIS could examine all of these matters if it was conducting an inspection of ASD's performance of its statutory cooperation functions with the AFP or ACIC.

Recommended improvements

304. The Law Council acknowledges that the Bill proposes to confer powers on the IGIS and Ombudsman to share information with each other.[106] To an extent, this may help to maintain some continuity of oversight in relation to the actions of ASD officials under the data disruption regime. However, information-sharing alone will not cure the risk that arbitrary differences and inconsistencies will arise in the nature and scope of oversight, depending on the precise legal mechanism by which ASD provides assistance to the AFP or ACIC with respect to data disruption operations.

305. The Law Council considers that the nature and scope of independent operational oversight over ASD should not be dependent on discretionary decision-making by the agencies subject to oversight, or their Ministers, about the technical legal basis upon which ASD staff members will provide assistance. Rather, the Law Council considers that there should be consistency of oversight responsibilities, functions and powers in all circumstances in which ASD staff members exercise, or enable the exercise of, 'offensive' powers to disrupt cybercrime within Australia.

306. The Law Council suggests that the most straightforward way of implementing this objective would be to amend section 8 of the IGIS Act to confer oversight function on the IGIS in relation to ASD staff members who are seconded to another agency for the purpose of executing an electronic surveillance warrant or authorisation, including data disruption.

307. This proposal would effectively give the IGIS and Ombudsman concurrent oversight jurisdiction over the relevant ASD staff members, in relation to their participation in data disruption and other electronic surveillance operations carried out by the AFP or ACIC. The IGIS and Ombudsman could then use their information-sharing powers to cooperate administratively to determine how best to manage overlap when overseeing individual operations.

[106] Bill, Schedule 2, item 71 (inserting new 32AC of the IGIS Act) and item 90 (inserting new section 35AB of the Ombudsman Act). These provisions replicate proposed amendments in the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020.

Recommendation 24—oversight of ASD's activities under disruption warrants

- **The IGIS Act should be amended to provide that, for the avoidance of any doubt, staff members of ASD are subject to IGIS oversight if they are seconded to the AFP or ACIC to execute a data disruption warrant for and on behalf of the AFP or ACIC (as applicable).**

Reporting requirements

308. Existing section 49 of the SDA requires the AFP and ACIC to furnish written reports to the Minister for Home Affairs, in relation to each surveillance device and computer access warrant issued, which provide details of the acts and things done under those warrants. These reports must be prepared and provided as soon as practicable after the relevant warrant ceases to be in force. In addition, existing section 50 of the SDA requires the Minister to prepare and table in Parliament annual reports on surveillance device and computer access warrants, providing largely statistical information about warrants sought, issued and executed during the previous financial year.

309. Proposed subsection 49(2D) and paragraph 50(1)(eb) (items 40-42 of Schedule 1) would extend these reporting requirements to data disruption warrants. The Law Council welcomes these reporting requirements, which will provide an important transparency measure in the exercise of the new powers. However, the Law Council considers that these reports should be required to include further information, as outlined below.

Ministerial reports on individual warrants

Content of warrant reports

310. The Law Council recommends that the requirements in proposed subsection 49(2D) are strengthened, so that the Minister is routinely informed of the exercise of the most intrusive powers under data disruption warrants. In particular, reports should be required to specifically inform the Minister of the following, additional matters:

- **enlivenment of immunities, where activities have interfered with the property rights of non-suspects, or are likely to do so**—warrant reports should be required to identify whether any acts were done in purported reliance on the authorisations in proposed subsection 27KE(7) or 27KE(10) (or both) to engage in acts that were likely to cause, or in fact caused, the following effects on a person who is lawfully using a computer:
    - material interference with, interruption to, or obstruction of the lawful use of a computer; or
    - material loss of, or damage to property (tangible or intangible)
- **comprehensive breach reporting**—warrant reports should be required to provide details of the agency's compliance with the statutory limits of authority under proposed section 27KE. This should be additional to the requirement in proposed subparagraph 49(2D)(d)(viii) for warrant reports to provide details of the agency's compliance with any warrant-specific conditions imposed by the relevant issuing authority. The Law Council has previously recommended

equivalent, comprehensive breach reporting requirements in relation to other intrusive powers conferred on security agencies;[107]

- **exercise of telecommunications interception powers**—warrant reports should be required to inform the Minister whether any telecommunications were intercepted under the data disruption warrant, and if so, the nature of the interception activities and their contribution to the effectiveness of the warrant operation. This will ensure that there is no diminution in the reporting requirements for interception activities that are authorised by an interception warrant issued under the TIA Act; and
- **extraterritoriality**—warrant reports should be required to inform the Minister whether any data disruption activities were undertaken outside Australia and, if so, details of steps taken by the AFP or ACIC to avoid duplication or conflict with the offshore cybercrime disruption functions of ASD under paragraph 7(1)(c) of the ISA. This should include the reasons it was considered more appropriate for the AFP or ACIC to exercise jurisdiction rather than ASD.

Reporting on post-warrant concealment activities

311. As noted in recommendation 13 above, the Law Council suggests that the AFP or ACIC should be required to obtain a separate, independent authorisation to carry out any post-warrant concealment activities specified in proposed subsection 27KE(9) more than 28 days after the relevant data disruption warrant has expired. By extension, the Law Council also considers that separate Ministerial reporting requirements should apply to those post-warrant concealment activities.

312. Even if recommendation 13 is not adopted, the Law Council recommends that there is a statutory reporting requirement for post-warrant concealment activities that are carried out after the report on the relevant disruption warrant has been submitted to the Minister. This recognises the highly intrusive and covert nature of the post-warrant concealment activities authorised under proposed subsection 27KE(9). A statutory requirement to report to the Minister as soon as practicable after those powers are powers are exercised would:

- create the strongest possible assurance that the Minister will be informed promptly of all intrusive powers that are authorised to conceal that actions were taken under a data disruption warrant; and
- provide a clear, consistent and transparent benchmark for independent oversight by the Ombudsman.

Recommendation 25—additional Ministerial reporting requirements

- **Proposed subsection 49(2D) of the SDA (item 40 of Schedule 1) should be amended to make provision for the following matters:**
  - **the reports of the AFP and ACIC to the Minster on each data disruption warrant must include the additional content listed at paragraph [310] of this submission; and**
  - **the AFP and ACIC must give the Minister a separate report on post-warrant concealment activities carried out under proposed subsection 27KE(9) if any such activities are carried out after a**

[107] See: Law Council of Australia, *Submission to the PJCIS Review of the Australian Security Intelligence Organisation Amendment Bill 2020*, (July 2020), 120-121 at [522]-[526] and recommendation 76 (concerning ASIO's powers to use tracking devices under internal authorisations only).

warrant report has been given to the Minister under proposed subsection 49(2D) of the SDA.

Aggregated annual reports on data disruption warrants

313. The Law Council further recommends that the content requirements for annual reports on data disruption warrants under section 50 of the SDA should be amended in line with the more detailed reporting requirements for individual warrant reports, as outlined above.

314. In particular, annual reports should provide aggregated statistical information about breaches of the limits of authority under a warrant, and the occasions on which the AFP or ACIC have caused material loss or damage to third parties who are lawfully using, or otherwise reliant on, a computer. These are likely to be the sources of the most intrusive and potentially harmful actions under the proposed data disruption regime. It is therefore important that the Parliament and the public are informed about the frequency of such actions during each financial year.

Recommendation 26—additional annual reporting requirements

- **Section 50 of the SDA (as amended by items 41-42 of Schedule 1) should be amended to require annual reports on data disruption warrants to provide aggregated statistical information on the matters identified in paragraph [310] of this submission, in relation to all data disruption warrants issued during the relevant financial year.**

Evidential issues in relation to data disruption warrants

315. Proposed section 65C of the SDA (item 51 of Schedule 1 to the Bill) provides that nothing in the SDA prevents evidence obtained from access to, or disruption of, data under a data disruption warrant or emergency authorisation from being admissible as evidence in a proceeding relating to a relevant offence.

316. This provision appears to convey a policy intention that any information obtained in the course of executing a data disruption warrant, including an act of data disruption itself, should be capable of being admitted in evidence in the prosecution of a person for the offence or offences covered by the warrant. This raises the possibility that data disruption warrants could lawfully be used for both disruptive purposes (in the sense of attempting to actively frustrating the commission of the offence via the disruption of data); and investigative purposes (in the sense of collecting admissible evidence of an offence to support a prosecution of that offence).

The risk of tainting evidence of an accused person's actions

317. There is a significant risk that a data disruption activity carried out under a disruption warrant may compromise the integrity and reliability of digital evidence of a suspect's alleged criminal actions that are carried out using a computer. Accordingly, the Law Council has grave concerns with a proposal that would:

- empower the AFP and ACIC to effectively tamper with potential evidence of an offence (that is, by disrupting data); and
- make it possible for that evidence to be admitted in the prosecution of a person for that offence.

318. The integrity of evidence admitted against a defendant in a criminal prosecution goes to the heart of a defendant's right to a fair trial. The Law Council considers it

imperative that the Bill contains an express exclusionary rule for evidence obtained under a data disruption warrant, so that it cannot be admitted in the prosecution of the relevant offence or offences covered by that warrant.

319. The Law Council acknowledges that various, existing exclusionary rules of evidence may potentially apply to information obtained under a data disruption warrant, if there is a suspicion that its integrity has been impaired by a data disruption activity. In particular, the court must exclude evidence adduced by the prosecution if satisfied that its probative value is outweighed by the danger of unfair prejudice to the defendant. The court may also exclude evidence if there has been impropriety, and not merely illegality, in its collection.[108]

320. However as detailed below, a defendant's ability to challenge the admissibility evidence on the basis it has been compromised by a data disruption activity is likely to be limited by several practical and legal constraints.

321. Moreover, it may not be technically possible to readily identify and quantify the impacts of a data disruption activity on the integrity, accuracy and reliability of evidence about the online activities of suspects and others. This reflects that data disruption activities may have potentially far-reaching evidentiary impacts on digital data, which may not have been foreseen, intended, or fully identified or understood when they were carried out (or subsequently). This is consistent with the principal objective of data disruption powers to covertly frustrate the commission of an offence, rather than to collect admissible evidence of a suspect's actions to enable their arrest, charge and prosecution.

Practical and legal difficulties in challenging evidence

322. If the prosecution adduces evidence obtained from the exercise of a warrant-based power of data disruption, the practical task of challenging that evidence on the basis of existing, general exclusionary rules of evidence may be impossible or complex.

323. Establishing the precise impacts of a data disruption activity on the integrity and reliability of digital evidence of a defendant's online or computer-related activities is likely to require detailed expert and forensic analysis and advice, and associated legal argument about the admissibility of that expert evidence, and the appropriate degree of weight it should be given. This is liable to consume extensive resources of the courts and all parties, including defendants who are reliant on legal aid.

324. Further, defendants who seek to challenge the admissibility of evidence obtained under a data disruption warrant, on the basis it has been compromised by a data disruption activity, may be at a significant legal disadvantage in attempting to do so. Several statutory mechanisms may apply, either individually or in combination, to prevent or limit their access to evidence of the data disruption activity.

325. In particular, the following mechanisms could be invoked at the instigation of the Commonwealth, either individually or in combination:

- proposed section 47B of the SDA (item 39 of Schedule 1) would entitle the Commonwealth to object to the disclosure of information, on the basis that it would reveal details of disruption technologies or methods. The trial judge would then need to hear further argument about whether the disclosure is necessary for the fair trial of the defendant under proposed subsection 47B(3).

[108] For example, in uniform evidence jurisdictions (Cth, NSW, VIC, TAS, NT and ACT), see sections 137 and 138 of the Uniform Evidence Law. Illustratively, these provisions are codified in sections 137 and 138 of the *Evidence Act 1995* (Cth).

Even if the trial judge ultimately ordered disclosure, it is conceivable that proposed section 47B would be invoked frequently in prosecutions involving evidence obtained under a data disruption warrant, and the process for resolving objections is likely to divert the resources of the court and parties;

- the Commonwealth Attorney-General may separately invoke the *National Security Information (Criminal and Civil Information) Act 2004* (Cth) in relation to evidence of the data disruption activities carried out under the disruption warrant; and

- an 'appropriate authorising officer' for the AFP or ACIC could issue an evidentiary certificate under section 62 of the SDA, in relation to anything done in connection with the execution of a warrant or emergency authorisation. This would be taken as prima facie evidence of those matters, which would place the onus on the defendant to challenge the matters in the certificate.

Further risks if ASD staff are engaged to perform acts of data disruption

326. A further concern may arise from the engagement of ASD staff members to execute data disruption warrants issued to the AFP or ACIC. As ASD is not a law enforcement agency, there is no guarantee that those staff members will possess the necessary expertise and experience in the collection of admissible evidence for the purpose of investigating and enforcing criminal offences.

327. As the case of *R v Ul-Haque* [2007] NSWSC 1251 made clear in relation to the intelligence collection activities of ASIO, as part of that agency's counter-terrorism investigations, there can be dire consequences for individual defendants and the viability of prosecutions if intelligence officers effectively perform evidence collection functions, without appropriate training about the requirements of evidence law.

328. In *R v Ul-Haque*, a prosecution for a terrorism offence was ultimately withdrawn after evidence of admissions by the accused to ASIO and AFP officers was ruled inadmissible due to the oppressive conduct of the ASIO officers who interviewed the accused person as part of a joint counter-terrorism operation by ASIO and the AFP. That conduct was held to be a 'gross breach of powers' by those officers, which resulted in the accused being subject to intimidation to participate in a 'voluntary' interview, and subsequently being falsely imprisoned.

329. A subsequent inquiry by the IGIS into ASIO's actions concluded that the relevant ASIO officers did not have sufficient knowledge or training to avoid their actions impacting on the gathering of admissible evidence by police.[109] While this case involved ASIO and not ASD, it clearly illustrates, at the level of principle, the risks that can arise when intelligence officers are required to engage in activities for, or in close connection with, law enforcement agencies.

330. The extrinsic materials to the Bill do not provide tangible assurances about any steps that have been, or will be, taken to mitigate the risk that any intelligence officers who are performing data disruption activities under the new form of warrant will have the requisite capabilities to simultaneously collect reliable and admissible evidence of the relevant offences.

331. Further, there is reasonable scope to doubt that it would be possible for **any official** executing a data disruption warrant to fully remove the risk that the data disruption activity or activities may contaminate evidence of alleged criminality by the suspect.

[109] IGIS, *Unclassified report of an inquiry into the actions taken by ASIO in 2003 in respect of Mr Izar Ul-Haque and related matters*, (2008), 51-52 at [198]-[202] and recommendation 5.

The Law Council is concerned that it may not be technically possible to avoid that risk, even in the case of a warrant that is executed solely by police and other law enforcement professionals who are trained and experienced in the collection of admissible evidence in criminal investigations.

An exclusionary rule for all information obtained under data disruption warrants

332. Accordingly, the Law Council is concerned about the combined effect of the serious risk that evidence will be tainted by a disruption activity, and the significant difficulty and complexity in challenging the admissibility of evidence on that basis. This will be exacerbated by the multiplicity of legislative tools available to the Commonwealth to prevent or restrict a defendant's access to detailed evidence about the disruption activity, for the purpose of ascertaining its impacts on the accuracy and reliability of evidence of an alleged offence that is carried out using a computer.

333. The Law Council therefore recommends that all information obtained under a data disruption warrant should be deemed inadmissible in a subsequent prosecution for a 'relevant offence' of the kind specified in the disruption warrant. Rather, law enforcement agencies should be required to elect between either:

- obtaining a data disruption warrant to enable them to actively frustrate the commission of a relevant offence or offences, via data disruption activities. (Any information obtained in the execution of the warrant would be inadmissible in criminal proceedings relating to the relevant offence or offences covered by the data disruption warrant); or
- obtaining a computer access warrant to enable them to collect admissible evidence of the offences, to facilitate the prosecution of a suspect or suspects for the relevant offence or offences. (Or in the further alternative, making subsequent use of intelligence obtained under a network activity warrant, or intelligence shared by ASIO under one of its computer access warrants.)

334. To avoid doubt, the Law Council would not oppose the ability of law enforcement officers to make **derivative use** of evidence obtained under a disruption warrant, for the purpose of obtaining admissible evidence that could be used to support a prosecution (for example, as the basis for requesting a computer access warrant).

335. A specific exclusionary rule for evidence obtained under a data disruption warrant, together with a use immunity, would be consistent with the approach proposed in Schedule 2 to the Bill in relation to network activity warrants (which authorise the AFP and ACIC to access data held in, or accessible from, a computer for the purpose of collecting criminal intelligence).[110]

Recommendation 27—specific exclusionary rule of evidence

Preferred option

- **Proposed section 65C of the SDA (item 51 of Schedule 1) should be omitted from the Bill and replaced with a provision stating that information obtained from the execution of a data disruption warrant is not admissible in criminal proceedings against a person for the relevant offence or offences specified in the data disruption warrant.**

Alternative (non-preferred) option

- **If the Law Council's primary recommendation is not implemented:**

[110] Bill, Schedule 2, item 19 (inserting proposed subsections 45B(3) and (10) of the SDA).

- **the Government should provide the Committee with information about the arrangements for the training, authorisation and supervision of ASD staff members to execute data disruption warrants, in the context of collecting admissible evidence;**
- **A staff member of ASD should not be made available to the AFP or ACIC, in any capacity, unless they have satisfactorily completed the above training and have complied with periodic re-accreditation requirements;**
- **the IGIS and Ombudsman should incorporate the matter of training and supervision of ASD staff members in the context of evidence collection activities into their respective agency inspection plans for ASD, the AFP and ACIC under the data disruption warrant regime;**
- **proposed section 47B of the SDA (item 39 of Schedule 1) should be omitted from the Bill; and**
- **there should be an independent review of the operation of proposed section 65C of the SDA, and the use of evidence obtained pursuant to data disruption warrants, after an appropriate period of time (indicatively, around three years after the commencement of proposed section 65C).**

Secrecy provisions for 'protected information'

The secrecy regime in sections 44 and 45 of the SDA

336. Existing section 45 of the SDA contains restrictive secrecy provisions in relation to the subsequent disclosure and use of 'protected information'. This is defined broadly in existing section 44 to cover:
    - information obtained under a warrant or an emergency authorisation;
    - information about the existence, issue or expiry of a warrant or an emergency authorisation; and
    - information about the existence of an application for a warrant or an emergency authorisation.
337. Existing section 45 prohibits the use, recording, communication and publication of protected information or its admission in evidence, unless an exception applies under subsection 45(4) or (5) for a prescribed 'permitted purpose'. The permitted purposes include the following circumstances:
    - the investigation of a relevant offence, including decision-making about whether or not to bring a prosecution;
    - inspections by the Ombudsman;
    - corruption and official misconduct investigations;
    - if the information that has already been lawfully disclosed in open court; and
    - if the disclosure and use is made for the purposes of ASIO or an ISA agency performing its functions.
338. Items 28-34 of Schedule 1 to the Bill propose to expand the definition of 'protected information' in section 44 to include information obtained under, or relating to the

existence, issue or expiry of data disruption warrants. Item 35 further proposes to expand the permitted disclosure exceptions in section 45 to enable Ombudsman officials to disclose protected information to IGIS officials, for the purpose of the IGIS performing their oversight functions.

Absence of permitted disclosures for the purpose of obtaining legal advice

339. The Law Council has previously raised concerns about inadequacies in the permitted disclosures in section 45 of the SDA.[111] In particular, there is no permitted disclosure for the purpose of a person obtaining legal advice about any matter relating to a warrant or an emergency authorisation issued under the SDA.

340. While existing paragraph 45(5)(c) enables disclosures to be made for the purpose of legal proceedings, the Law Council notes that a person may need to obtain legal advice for purposes separate to litigation or prosecution. For example, a person may need to seek legal advice if a warrant operation becomes overt to them (whether intentionally or otherwise) and they are adversely affected by the activities undertaken in purported reliance on the warrant.

341. The Explanatory Memorandum expressly contemplates the possibility that the AFP or ACIC may choose to make a warrant operation known to certain individuals. It refers to circumstances in which the AFP or ACIC seek to compel the assistance of a suspect or another person with relevant knowledge of a computer to execute the data disruption warrant, or to make intelligible data obtained under such a warrant, by obtaining a separate compulsory assistance order under proposed section 64B of the SDA (discussed below). The Explanatory Memorandum states that 'there may be a point in the investigation where the benefits of compelling information from a person … outweigh the disadvantages of maintaining the secrecy of the investigation'.[112]

342. However, the restrictive secrecy provisions of the Bill, as presently drafted, would mean that a person who is served with a compulsory assistance order would not have a clear and comprehensive legal basis upon which to obtain legal advice about their rights or obligations. The same observations would apply if the AFP or ACIC disclosed the existence of a warrant operation to any other person, for any other reason, or if the warrant operation unintentionally became overt to another person.

343. The Law Council considers that the novel and high-risk nature of data disruption activities necessitates amendments to section 45 of the SDA, to enable disclosures of protected information to a lawyer, for the purpose of obtaining legal advice, or initiating legal proceedings. This should also cover dealings with protected information (such as making records or copies or taking extracts) in preparation for disclosing it to a lawyer in order to obtain legal advice in connection with the warrant, or acts done under the warrant.

344. It is also important to acknowledge that the proposed power of data disruption will significantly increase the risk that third parties who are not under any suspicion of wrongdoing could suffer material loss, damage or interference with their lawful activities. This is particularly because proposed subsections 27KE(7) and 27KE(9) will permit activities that cause material loss or damage in certain circumstances, based on a self-assessment by the AFP or ACIC that the result is 'justified'. That is, the AFP or ACIC will be the sole arbiter of whether they are authorised to cause

[111] See, for example: Law Council of Australia, *Supplementary Submission to the PJCIS Review of the TOLA*, (August 2020), Attachment 1 at 23 (citing matters raised in multiple, previous submissions of the Law Council to inquiries into the TOLA Bill and subsequently the TOLA Act).

[112] Explanatory Memorandum, 56 at [239].

material loss or damage to a third-party, in advance of engaging in the relevant acts. A person who sustains the loss or damage would necessarily need to make a complaint or commence proceedings seeking compensation after the event.

345. The Law Council considers that this risk of serious harm or damage, and the fact that law enforcement agencies can effectively self-determine whether they are entitled to cause such results, should be reflected in an expansion of the permitted purposes for disclosure. Section 45 of the SDA should make explicit that any person can disclose protected information to their lawyer, for the purpose of obtaining legal advice in relation to a data disruption warrant. The SDA should remove any scope for doubt or uncertainty about the legality of such disclosure.

346. The Law Council considers that the permitted disclosure provisions should be extended in this way for 'protected information' in connection with all of the types of warrants and authorisations issued under the SDA (namely, in relation to surveillance devices, computer access, data disruption, network activity and account takeover). However, as an absolute minimum, it must cover data disruption, given the particularly high risk that third parties will suffer serious loss or damage as a result of data disruption activities.

Recommendation 28—permitted disclosures in relation to legal advice

- **The Bill should further amend section 45 of the SDA to insert a permitted purpose for the disclosure of protected information (and preparatory dealings with that information). This should cover disclosures for the purpose of obtaining legal advice, or initiating legal proceedings, in connection with a warrant or emergency authorisation, or acts done under the warrant or emergency authorisation.**
- **This new ground of 'permitted disclosure' should apply to <u>all types</u> of warrants and emergency authorisations under the SDA. However, as an absolute minimum, it should cover data disruption warrants and emergency authorisations for data disruption.**

Mandatory assistance orders for data disruption (Schedule 1)

347. Schedule 1 to the Bill also proposes to insert new section 64B in the SDA to establish a regime of mandatory assistance orders in relation to the execution of data disruption warrants, or emergency authorisations for data disruption.

348. These orders are equivalent to mandatory assistance powers available to the AFP and ACIC, which were extended or enacted by the TOLA Act in 2018, namely:

- existing section 3LA of the Crimes Act (in relation to data obtained from computers that were accessed under search warrants); and
- existing section 64A of the SDA (in relation to data obtained from computers that were accessed under computer access warrants).

349. Proposed section 64B establishes an equivalent regime for data disruption warrants. Specifically, it would enable a 'law enforcement officer' of the AFP or ACIC to make an application to an eligible judge or a nominated AAT member ('issuing authority') for an order to compel any person to provide any information or assistance to allow a law enforcement officer to do any or all of the following activities, in relation to data held in a computer that is covered by a data disruption warrant or an emergency authorisation:

- disrupt data;
- access data;
- copy data; and
- convert data into documentary form, or another form that is intelligible to a law enforcement officer.[113]

350. It is conceivable that a compulsory assistance order could be sought and obtained simultaneously with the issuance of a data disruption warrant. The persons who are eligible for appointment as issuing authorities for mandatory assistance orders cover the same classes of persons who are eligible for appointment as issuing authorities for data disruption warrants.[114] It is therefore possible that the Attorney-General may appoint individuals as issuing authorities for both powers.

351. The issuing authority may grant the order if satisfied that it is likely to substantially assist in frustrating the commission of the relevant offences covered by the warrant, and is justifiable and proportionate.[115] If an order is sought in relation to an emergency authorisation, the issuing authority must also be satisfied that there is an imminent risk of serious violence or substantial property damage, and data disruption is necessary for the purpose of dealing with that risk.[116]

352. Compulsory assistance orders may be issued against the following persons, if they have 'relevant knowledge' of the computer or a network to which it is connected, or measures applied to protect data held in the computer:

- a suspect in relation to any of the relevant offences covered by the warrant;
- the owner or lessee of the computer, or their employees or contractors;
- a person who uses or has used the computer; and
- a person who is a system administrator for a system that includes the computer.[117]

353. The Bill proposes to enact an offence for persons who fail to comply with an order by omitting to do a required act, which they are capable of doing. It is punishable by a maximum penalty of 10 years' imprisonment or 600 penalty units ($133, 200) or both penalties.[118]

354. Proposed section 64B does not prescribe any statutory maximum period of effect for mandatory assistance orders. Nor does it prescribe any requirements as to the form of orders or applications, service on persons subject to orders, 'per-use' and annual reporting obligations in relation to orders, record-keeping requirements equivalent to the register of warrants that must be maintained under the SDA, or notification of oversight bodies of the issuance and execution of orders.

[113] Bill, Schedule 1, item 47 (inserting proposed subsection 64B(1) of the SDA).

[114] Ibid (inserting proposed subsection 64B(1) of the SDA, which refers to an 'eligible judge' or 'nominated AAT' member as defined in existing sections 12 and 13 of the SDA).

[115] Ibid (inserting proposed paragraph 64B(2)(a) of the SDA).

[116] Ibid (inserting proposed paragraph 64B(2)(b) of the SDA).

[117] Ibid (inserting proposed paragraph 64B(2)(e) of the SDA).

[118] Ibid (inserting proposed subsection 64B(3) of the SDA).

Appropriateness of compulsory assistance powers for disruption

The need for justification of the power to compel others to perform data disruption

355. The Law Council is concerned that the extrinsic materials to the Bill do not provide any justification for the power to compel a third-party (including non-suspects) to executive a disruption warrant by performing a data disruption activity.

356. The power to compel data disruption is materially different to the present power to compel other forms of assistance under the existing mandatory assistance orders for search warrants under the Crimes Act and surveillance device and surveillance device and computer access warrants under the SDA. The existing forms of assistance which can be compelled are limited to accessing, copying and making intelligible data. They necessarily do not cover 'offensive' data disruption activities that actively involve the frustration of an offence by means other than arrest and charge (or obtaining other orders to confiscate or freeze assets).

357. The Richardson Review expressly rejected proposals to confer a statutory data disruption power directly on the AFP or any other law enforcement agency. A power to compel private persons to perform data disruption activities, at the behest of the AFP or ACIC, is an even more extraordinary proposition.

358. This is particularly the case for owners or lessees of computers, or system administrators, who may be compelled to carry out data disruption activities against their own infrastructure. Such an order could potentially be used to compel these persons to inflict significant loss on, or damage to, their own commercial or other interests. The trigger for such compulsion would be the self-assessment by the AFP or ACIC under proposed paragraph 27KE(7)(b) that the causation of material loss or damage, via the intended act of data disruption, was 'justified' in the circumstances.

359. A person who refused to carry out an act of data disruption in these circumstances would commit an offence under proposed section 64B and would be exposed to up to 10 years' imprisonment, provided that they were technically capable of carrying out the relevant act. There would be no defence or excuse to accommodate the fact that the person was being compelled to cause material loss or damage to themselves (or others); or that they reasonably believed that the causation of such loss or damage was not necessary, reasonable or proportionate (for example, because they knew of, and were prepared to assist with implementing, less injurious alternative technical solutions).

Overbreadth in the persons who may be compelled to perform data disruption

360. Mandatory assistance orders compelling private persons to perform data disruption activities can be sought against an extremely wide class of persons, which far exceeds suspects in relation to the offences covered by a data disruption warrant. Proposed section 64B would enable a compulsory assistance order to be issued against anyone who uses (or has used), owns or leases a computer covered by the warrant; or is employed by or contracted to the owner or lessee; or is a system administrator in relation to the relevant computer system or network.

361. Significantly, the term 'computer' is defined extremely broadly in section 6 of the SDA to extend its ordinary meaning, by covering multiple individual devices, systems or networks, or any combination of these. For example, the entire computer network of a university or corporation could be a single computer. In such cases, any user of a device that is connected to such a network could be the subject of a mandatory assistance order, provided that they have the requisite technical

knowledge to disrupt or access data. This could be knowledge of general application, which could be utilised to disrupt or access data held on any computer.

362. The Explanatory Memorandum states that there is currently no subjective policy intention for compulsory assistance orders to be obtained to compel the communications industry to carry out data disruption activities.[119] As the Bill contains no legal safeguards to prevent this from occurring, this objective will be solely reliant on individual law enforcement officers exercising their discretion, in each and every request for a compulsory assistance order, to act consistently with the expression of policy intent.

363. For example, under the Bill as currently drafted, it would be legally possible to obtain a compulsory assistance order against a data storage provider that is contracted to provide services to a company, or the system administrator for a corporate or institutional network that unwittingly hosts an online forum used to disseminate unlawful content. Such persons could be exposed to significant criminal penalty if they are capable of performing the act or acts of disruption sought, but declined to comply with the order, even if it would have severe impacts on their own business.

364. This undermines the assurance provided in relation to a separate legislative proposal in the Security Legislation Amendment (Critical Infrastructure) Bill 2020. That Bill includes a provision to the effect that the proposed powers in the *Security of Critical Infrastructure Act 2018* (Cth) (**SCI Act**) to enable government intervention in serious cyber-security incidents affecting private critical infrastructure assets (including by issuing directions to take specified action) could not be used to direct an owner or operator of an asset to perform 'offensive' cyber activities.[120] In fact, a data disruption warrant and an accompanying mandatory assistance order could be obtained and executed simultaneously with a Ministerial Authorisation for intervention under the SCI Act.

365. A bare statement of subjective policy intent at a given point in time, before the proposed data disruption regime has commenced operation, does not provide any meaningful assurance against individual law enforcement officers subsequently deciding to exercise their discretion to use the powers in a contrary manner. There is reasonable scope for doubting that law enforcement agencies engaged in the investigation of cyber-enabled crime would be in a position to recall a statement of policy intent that is contained in a single line of an explanatory memorandum to an amending Bill. A legal safeguard, which prohibits any such compulsion, is needed to give effect to the policy intent.

366. The absence of any statutory implementation of the policy intent referred to above also has the potential to undermine crucial public trust and confidence in the AFP and ACIC. If the Bill is passed in its present form, and either of those agencies acted inconsistently with the stated policy intent in relation to the use of compulsory assistance orders, they may be exposed to significant public criticism for acting inconsistently with the assurances provided by the Government in the Explanatory Memorandum (on which members of the Parliament may have placed weight in deciding to pass the Bill). Accordingly, the inclusion of the statutory safeguards recommended below would also provide clarity and certainty to the AFP and ACIC about the circumstances in which powers of compulsion should be exercised.

Recommendation 29—removal of power to compel assistance for data disruption

[119] Explanatory Memorandum, 56 at [238].

[120] Security Legislation Amendment (Critical Infrastructure) Bill 2020, Schedule 1, item 45 (inserting proposed paragraph 35AB(9)(b) of the SCI Act).

- **The Bill should be amended to provide that mandatory assistance orders under proposed section 64B of the SDA (item 47 of Schedule 1) cannot compel a person to carry out acts of data disruption, which are authorised by a data disruption warrant or an emergency authorisation for data disruption.**

Issuing authorities and issuing process

367. For the same reasons outlined above in relation to issuing authorities for data disruption warrants, the Law Council considers that the power to issue accompanying mandatory assistance orders should also be limited to superior court judges who are appointed in their personal capacities.

368. Given that the execution of a mandatory assistance order will necessarily make the relevant disruption operation overt to the subject of that order, the Law Council considers that there should also be an opportunity for applications for those orders to be heard on an *inter partes* basis.

369. This would enable the person, or persons, who are subject to a proposed assistance order to provide information about their technical capabilities and the impacts of the proposed order, to inform a decision under proposed paragraph 64B(2)(a) as to whether the assistance sought is likely to be effective, and would be justified and proportionate. It is otherwise conceivable that law enforcement applicants will not have the information necessary for the issuing authority to make an assessment that takes account of all relevant considerations.

370. The Law Council recommends that there should be a default position in favour of *inter partes* applications, unless a specified exception applies, such as on the grounds of urgency, prejudice to an operation (such as the risk of tip-off) or risks to the life or safety of another person. If an application is determined *ex parte,* there should be a requirement for a public interest advocate (as recommended above in relation to the issuance of disruption warrants) to act as a contradictor.

Recommendation 30—issuing authorities and issuing process for mandatory assistance orders in relation to data disruption warrants

- **Proposed section 64B of the SDA (item 47 of Schedule 1) should be amended as follows:**
  - **only superior court judges (appointed in their personal capacity) should be able to issue a mandatory assistance order, consistent with the Law Council's recommendations on disruption warrants;**
  - **applications for such orders should be conducted *inter partes*, unless a prescribed exception exists, on the grounds of urgency, or risks of prejudice to an operation or safety and security; and**
  - **if an application is conducted on an *ex parte* basis, public interest advocates, as recommended above in relation to disruption warrants, should be appointed to act as contradictors.**

Issuing criteria

‘Necessity’ v ‘substantial assistance’ of compulsory assistance

371. In the case of compulsory assistance orders issued in relation to data disruption warrants, there is no issuing criteria that requires the compulsion of assistance to be **necessary** for the purpose of ‘frustrating’ the commission of a ‘relevant offence’.

372. Rather, proposed paragraph 64B(2)(a) applies the thresholds of ‘substantial assistance’ and ‘justifiable and proportionate’ having regard to the relevant offences covered by the warrant. The Explanatory Memorandum provides no justification for the selection of the lower threshold of ‘substantial assistance’ rather than ‘necessity’.

373. The Law Council considers that, if compulsory assistance orders are to be available for data disruption warrants or emergency authorisations, then such orders should be subject to an issuing threshold of necessity. This reflects the extraordinary nature of the power of data disruption (as opposed to surveillance or computer access), in combination with an even more extraordinary power to compel private individuals to carry out the act of disruption (potentially including causing major interference and loss to their own commercial or other activities) at the request of the AFP or ACIC.

Assessment of proportionality

374. In addition, proposed paragraph 64B(2)(b) provides that the proportionality of a proposed assistance order is to be assessed by reference to the ‘relevant offences’ that are covered by the data disruption warrant.

375. The Law Council is concerned that this does not directly or clearly communicate to law enforcement applicants and issuing authorities the full scope of a proportionality assessment. This includes the need to consider the impacts of the proposed data disruption activities on third parties, including the subject of the compulsory assistance order or associated entities (such as their employer or clients).

376. It would be preferable for proposed section 64B to provide expressly that the assessment of proportionality requires consideration of the third-party impacts of compelling assistance. This will ensure that such matters are routinely and consistently considered. Otherwise, the consideration of such impacts would be reliant on the discretion of law enforcement officers in individual cases; or being prescribed in internal operational policies of the AFP and ACIC, which may not be available to the public, and could be changed or repealed unilaterally at any time.

Recommendation 31—necessity and proportionality requirements

- **If compulsory assistance orders are to be available in respect of data disruption warrants or emergency authorisations, then the issuing criteria in proposed paragraph 64B(2)(a) of the SDA (item 47 of Schedule 1) should be amended. An issuing authority should only be able to make an order if satisfied, on reasonable grounds, of the following matters:**
  - **compelling a person to carry out an act of data disruption is necessary to frustrate the commission of the relevant offence or offences that are covered by the data disruption warrant; and**
  - **the compulsion of that assistance is justifiable and proportionate, having regard to the relevant offences as well as**

the likely impacts of the data disruption activity on:

- **the person who is subject to the order, and any related parties (such as their employer, or the entity to whom the person is providing services under a contract); and**
- **other persons, including lawful computer users or clients of the person subject to the order, who may be adversely affected by the data disruption activity.**

Requirements for orders

Maximum period of effect and compliance period

377. Proposed section 64B does not specify a maximum period of effect for a compulsory assistance order, during which time it must be served on the relevant person.

378. The Law Council considers that this period cannot simply be implied from the duration of the underlying data disruption warrant, while it is in force. This reflects that some of the assistance that can be compelled, in relation to copying or making intelligible data that has been obtained under a disruption warrant, is capable of being rendered **after** that warrant has ceased to be in force. (Rather, the relevant data need only have been obtained under the warrant while it was in force.) As a technical matter of statutory interpretation, this factor tends against a 'necessary implication' that the period of effect of an assistance order is simply the period of effect for the disruption warrant.

379. In any event, a data disruption warrant can be in force for up to 180 days in total. Consequently, any linkage of the maximum duration for a compulsory assistance order to the total duration of the underlying data disruption warrant is too uncertain, and potentially disproportionately long, for a coercive power that can require individuals to engage in conduct which may cause serious harm to their own interests, and the interests of other parties such as their clients, under penalty of up to 10 years' imprisonment if they refuse to do so.

380. In view of the extraordinary and coercive nature of the powers under compulsory assistance orders, the Law Council considers that these orders should be subject to a maximum period of effect of seven days from the issuing of the assistance order, which is equivalent to the period of effect for law enforcement search warrants in the Crimes Act, which is seven days from the issuing of the assistance order.[121]

381. This would mean that a compulsory assistance order must be served on the subject within seven days after the day of issue. The issuing authority should be required to determine a compliance period that is necessary, reasonable and proportionate to the nature of the assistance sought in the particular circumstances, and the order should be issued subject to a condition prescribing that compliance period.

Form, service and key particulars

382. The Law Council considers that proposed section 64B and associated provisions of the SDA should also specify requirements for:

- the form in which all applications and orders must be made; and
- requirements for the service of orders on the relevant person(s); and

[121] Crimes Act, subsection 3E(5A).

- the key particulars that must be included in all applications and orders.

383. This should include the following requirements, which are important to enable a person to ascertain the nature and scope of their obligations and potential exposure to criminal liability:

- applications and orders must be made in writing (potentially subject to a provision for oral issuing, with record-keeping requirements, in defined circumstances of emergency, where proceeding orally is strictly necessary);
- an order must be served on the person to whom it is issued. The law enforcement officer serving the order should be subject to an explicit obligation to take all reasonable steps to ensure that the person understands the order, including their exposure to criminal liability for non-compliance;
- there should be an express provision stating that, to avoid any doubt, an order does not commence unless and until it is served on the person; and
- an order must specify:
  - the assistance that is required to be provided;
  - the way in which that assistance must be provided, or ways in which it may be provided;
  - the time at which, or by which, the assistance must be provided (which must be assessed by the issuing authority as being necessary, reasonable and proportionate, having regard to the nature of assistance sought to be compelled);
  - if a person is required to attend at a place to render the assistance, that place must be specified in the order;
  - that the person has a right to make a complaint to the Ombudsman in relation to the service and execution of the order;
  - the existence and effect of the offence in proposed subsection 64B(3) for non-compliance; and
  - the name and contact details of a liaison officer with the AFP or ACIC, should the person wish to discuss the order.

384. The Law Council further considers that proposed section 64B should provide expressly that an assistance order authorises only one instance of the specified act of assistance, such as a data disruption activity. It should be made explicit that a single order is not capable of authorising the repetitive provision of assistance over a period of time. For example, it should expressly exclude the possibility for repeated requests over the entire period of effect of an underlying disruption warrant, such as progressive requests to make 'tranches' of data intelligible to the AFP or ACIC; or to carry out the same or substantially similar acts of data disruption on multiple occasions. Rather, each individual act of assistance must be the subject of a specific application to the issuing authority for an order under new section 64B.

385. Statutory prescription of this matter is important because the authority conferred under the relevant data disruption warrant need not be limited to a single instance of each act or thing specified in proposed subsection 27KE(2) (such as data disruption, access to data, or telecommunications interception). Rather, multiple acts can be authorised while the warrant is in force (up to 180 days in total).

386. The Law Council notes that the existing provisions governing compulsory assistance orders for search warrants (in section 3LA of the Crimes Act) and computer access warrants (in section 64A of the SDA) do not contain the requirements listed above. However, it should not be assumed that these provisions provide acceptable precedents in any context, or that they are adequate in respect of compulsory assistance in relation to search, surveillance and computer access warrants.

387. In fact, the Law Council has previously made similar recommendations to remediate the same problems in section 3LA of the Crimes Act and section 64A of the SDA, as part of the multiple reviews of the TOLA amendments in 2018.[122] These issues remain outstanding. The Law Council continues to urge amendments to existing section 3LA of the Crimes Act and existing section 64A of the SDA, in addition to proposed section 64B of the SDA.

Recommendation 32—requirements for writing, service and key particulars

- **Proposed section 64B of the SDA (item 47 of Schedule 1) should be amended to impose the requirements set out at paragraphs [382]-[384] of this submission, with respect to:**
  - **a statutory maximum period of effect for orders, during which time they must be served and executed, or will lapse if this does not occur;**
  - **a prohibition on a single compulsory assistance order purporting to compel the repetitive provision of a specified act of assistance on multiple occasions over a period of time; and**
  - **requirements in relation to:**
    - **the form in which orders and applications must be made (namely, in writing);**
    - **the inclusion of key particulars in all orders (including specification of a compliance period or deadline); and**
    - **obligations for service of orders on the specified person (with the commencement of an order and compliance timeframes tied to the date and time of service).**

Implementation of safeguards recommended by the third INSLM

388. In his 2017 report on the TOLA Act, the third INSLM recommended that all compulsory assistance orders under the Crimes Act and SDA (and equivalent orders under the ASIO Act) should be subject to an express provision stating that nothing in those orders 'authorises the detention of a person to whom the order applies'.[123]

389. The third INSLM concurred with the Law Council, IGIS and other submitters who expressed concern that a requirement in a compulsory assistance order to attend premises to render assistance could amount to an arbitrary deprivation of liberty (including detention) under international human rights law. The third INSLM

[122] See, for example, Law Council, *Supplementary Submission to the PJCIS Review of the TOLA*, (August 2020), Attachment 1, 30 (citing matters raised in the Law Council's previous submissions).

[123] Dr James Renwick SC, INSLM, *Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, (30 June 2020), recommendations 17 and 23.

considered that this risk could arise if a person had reason to believe that they would not be free to leave the premises without rendering assistance, if they sought to do so. This may include because they would be under pain of a significant criminal penalty; or because the persons executing the order may physically obstruct exit points by guarding or locking them.[124]

390. These recommendations remain outstanding. The Law Council continues to support their implementation in respect of all types of mandatory assistance orders, including the new orders in proposed section 64B of the SDA.

391. As an additional safeguard, the Law Council considers that the AFP Commissioner and ACIC CEO should be subject to a related statutory obligation to take all reasonable steps to ensure that a person who is required under a compulsory assistance order to attend a specified place to render assistance is treated in a manner compatible with their status as a person who is not being detained.

392. This would place a positive, legal obligation on these agency heads to ensure that their respective agencies have adopted policies, systems and practices to comply with the requirement that mandatory assistance orders do not authorise detention; and must not be executed in a manner that amounts to detention (irrespective of whatever subjective statutory label that may be given to the deprivation of liberty).

Recommendation 33—implementation of third INSLM recommendations

- **Proposed section 64B of the SDA (item 47 of Schedule 1) should be amended to:**
  - **implement the recommendations of the third INSLM about mandatory assistance orders under section 64A of the SDA and section 3LA of the Crimes Act. Namely, there should be an express provision prohibiting a mandatory assistance order from authorising, or being executed in a manner that amounts to, the detention of a person; and**
  - **impose a related obligation on the AFP Commissioner and ACIC CEO, to take ensure that their agencies have implemented adequate arrangements to enable their compliance with this prohibition in executing all mandatory assistance orders.**

Oversight, record keeping and reporting requirements

Independent operational oversight by the Commonwealth Ombudsman

393. Proposed section 49C of the SDA (item 41 of Schedule 1 to the Bill) requires the AFP or ACIC to notify the Ombudsman of any act or thing done under a disruption warrant, within seven days. However, this requirement does not extend to any associated compulsory assistance orders issued under proposed section 64B. There do not appear to be any existing provisions of the SDA that would require the AFP or ACIC to notify the Ombudsman of such orders.

394. This anomaly should be rectified. The need for prompt, pro-active notification to help focus independent oversight applies equally to acts done under data disruption warrants, and assistance that is compelled to enable the execution of those warrants, or the examination and use of any data that is obtained under the authority of those warrants. There is no rational reason for singling out warrants for

[124] Ibid, 255-257 at [12.125]-[12.134].

notification obligations, to the exclusion of assistance orders that can compel private individuals to do the acts or things that are specified in the warrant, as well as providing ancillary support or assistance.

395. The Law Council notes that the existing inspection functions of the Ombudsman under Division 3 of Part 6 of the SDA are sufficiently broad to cover the compliance by the AFP and ACIC with the limits of authority under mandatory assistance orders, as well as warrants. This makes it particularly important that proposed section 49C is amended, or a separate provision inserted, to require notification of associated mandatory assistance orders. This will enable periodic inspections to comprehensively examine all of the extraordinary powers that have been exercised in a data disruption operation, irrespective of the particular legal instrument which conferred those powers.

396. The Law Council's comments at paragraphs [289]-[292] and recommendation 22 above, in relation to the expansion of the Ombudsman's inspection function beyond assessing agencies' strict legal compliance with the requirements of the SDA, apply equally to its inspections of mandatory assistance orders as well as warrants.

397. Moreover, to avoid doubt, the Law Council considers that the Division 3 of Part 6 of the SDA should be amended to make explicit that the Ombudsman has the power to enter premises, for the purpose of inspecting the execution of a compulsory assistance order that compels a person to attend specified premises to render the assistance or provide the information specified in the order. This power is important to the effective, independent oversight of orders of this kind, given that they create a risk of arbitrary detention or other deprivation of liberty (as noted by the third INSLM, whose findings and recommendations on this point are summarised above).

Recommendation 34—Ombudsman oversight of mandatory assistance orders

- **Proposed section 49C of the SDA (item 41 of Schedule 1) should be amended, or an equivalent provision inserted, to require the AFP and ACIC to notify the Ombudsman of the execution of a compulsory assistance order issued under proposed section 64B, in addition to requirements to provide notification about acts or things done under a data disruption warrant.**
- **The Ombudsman's inspection powers in Division 3 of Part 6 of the SDA should be amended to confer an express, discretionary power on the Ombudsman (and staff) to enter premises and be present during the execution of a mandatory assistance order issued under proposed section 64B, which compels a person to attend a specified place to render the assistance sought.**

Record keeping and reporting requirements

398. The provisions of Schedule 1 to the Bill and existing provisions of the SDA impose record keeping and reporting requirements in relation to warrants and emergency authorisations including data disruption. However, they do not cover related compulsory assistance orders such as those under proposed section 64B.

399. For example, the register of warrants that is required to be maintained under existing section 53 of the SDA does not require any notation to be made if a compulsory assistance order was issued in relation to that warrant (including to compel a private individual to do an act or thing authorised under the warrant, such accessing data held in a computer). The Bill does not propose to amend section 53 to include any such requirement in relation to compulsory assistance orders for data

disruption under proposed section 64B (for example, if a private individual is compelled to perform the data disruption activity authorised under the warrant, or provide other assistance to the AFP or ACIC to enable them to disrupt data).

400. Further, the Ministerial reporting requirements on each disruption warrant or emergency authorisation in proposed subsection 49(2D) (item 40 of Schedule 1) does not require the Minister to be informed of any associated compulsory assistance orders under proposed section 64B. There are also no requirements in relation to the annual reporting on compulsory assistance orders in section 50.

401. The Law Council considers that the interests in transparency and accountability, which underpin the reporting requirements on warrants, apply equally to compulsory assistance orders issued in connection with those warrants.

402. The differential treatment of warrants and associated assistance orders for reporting purposes is artificial and arbitrary. It also has the potential to provide the Minister, the Parliament and wider public with a misleading impression about the nature and extent of an agency's activities in warrant operations. This should be rectified in relation to all warrant types and associated assistance orders, including but not limited to data disruption.

Recommendation 35—enhanced record-keeping and reporting requirements

- **The Bill should be amended to:**
  - **extend the Ministerial reporting requirements in section 49 of the SDA, and annual reporting requirements in section 50 of the SDA, to cover mandatory assistance orders issued in relation to warrants or emergency authorisations; and**
  - **require the register of warrants and emergency authorisations under section 53 of the SDA to include details of any mandatory assistance orders issued in respect of each warrant or emergency authorisation.**

Network activity warrants (Schedule 2)

Overview of regime

403. Schedule 2 to the Bill contains the second of the three new powers. It proposes to enact the regime of 'network activity warrants' in new Division 6 of Part 2 of the SDA. These warrants would authorise the AFP and ACIC to remotely access data that is held in, or is accessible from, a computer for the purpose of collecting intelligence about a 'criminal network of individuals'.[125] This is defined as a group of individuals who are:

- 'electronically linked'[126] in that they use the same electronic service to communicate; and

[125] Bill, Schedule 2, Part 1 (inserting new Division 6 of Part 2 of the SDA). See especially item 8, which inserts the definition of a 'criminal network of individuals' in new section 7A. Broadly, this covers an 'electronically linked group of individuals, where one or more of those individuals have engaged in, or facilitated others to engage in, conduct which constitutes a 'relevant offence' within the meaning of section 6 of the SDA; or are likely to do so in future.

[126] Ibid, Schedule 2, item 3 (inserting the definition of an 'electronically linked group of individuals in section 6 of the SDA).

- have engaged, are engaging, or are likely to engage in conduct that constitutes a 'relevant offence' within the meaning of section 6 of the SDA (as discussed above in relation to data disruption warrants, and essentially covering Commonwealth offences punishable by a maximum penalty of at least three years' imprisonment); or
- have facilitated, are facilitating or are likely to facilitate the engagement by another person (who may or may not be a member of the group) to engage in conduct that constitutes a 'relevant offence'.[127]

404. As with data disruption warrants, and existing surveillance device and computer access warrants, the issuing authorities for network activity warrants are 'eligible judges' (judges of a federal court) or AAT members, who have consented to being appointed by the Attorney-General.[128] A network activity warrant may only be issued if the issuing authority is satisfied that there are reasonable grounds for the applicant's suspicion that:

- a group of individuals is a 'criminal network of individuals'; and
- access to data held in a computer (target computer) that is, from time to time, used, or likely to be used, by any of the individuals in the group will substantially assist in the collection of intelligence that:
  - relates to the group or any of the individuals in the group; and
  - is relevant to the prevention, detection or frustration of one or more kinds of 'relevant offences'.[129]

405. A network activity warrant may have a maximum duration of 90 days, subject to extension for up to a further 90-day period (180 days in total).[130] Network activity warrants authorise the same activities as for computer access warrants (including access to premises, the power to remove computers and other things from premises, and the power to intercept telecommunications).[131] However they also propose to authorise the use of surveillance devices (without a separate warrant) for the purpose of doing any other act or thing that is authorised under the network activity warrant.[132] This is not able to be authorised under the existing computer access warrant regime for the AFP or ACIC, or for ASIO.[133]

406. Schedule 2 to the Bill also proposes to establish a regime of mandatory assistance orders in relation to network activity warrants.[134] This is similar to the regimes in existing section 3LA of the Crimes Act (for search warrants), existing section 64A of the SDA (in relation to computer access warrants), and proposed section 64B of the SDA (in relation to data disruption warrants, per Schedule 1 to the Bill).

407. This would enable the AFP or ACIC to obtain an order from the issuing authority to compel the suspect, or others with relevant knowledge of the computer network or data protection measures (such as computer owners or system administrators), to render assistance in accessing data, or making intelligible data that has already been accessed under a warrant. Failure to comply with an order, where a person is

[127] Ibid, Schedule 2, item 8 (inserting proposed section 7A of the SDA).
[128] Ibid, Schedule 2. Item 9 (inserting proposed subsection 27KK(3) of the SDA).
[129] Ibid, Schedule 2, item 9 (inserting proposed subsections 27KM(1) and 27KK(1) of the SDA).
[130] Ibid, Schedule 2, item 9 (inserting proposed subsections 27KN(2) and 27KQ(1) of the SDA).
[131] Ibid, Schedule 2, item 9 (inserting proposed section 27KP of the SDA).
[132] Ibid, Schedule 2, item 9 (inserting new paragraph 27KP(2)(i) of the SDA).
[133] SDA, subsection 27D(1) and ASIO Act, subsection 25A(4).
[134] Bill, Schedule 2, item 31 (inserting new subsection 64A(6) of the SDA).

capable of rendering assistance, is an offence punishable by a maximum penalty of 10 years' imprisonment.

Distinction between criminal intelligence collection and investigation powers

408. The intelligence collection powers of the AFP and ACIC under network activity warrants would be additional to their investigative powers under the existing regime of computer access warrants in Division 6 of Part 2 of the SDA (enacted by the TOLA Act in 2018). Computer access warrants authorise the AFP and ACIC to access data that is held in, or is accessible from, a computer for the purpose of investigating and collecting admissible evidence about the suspected commission of a 'relevant offence' within the meaning of section 6 of the SDA.

409. The proposed regime of network activity warrants would invest the AFP and ACIC with similar computer access powers to those of ASIO under the ASIO Act for intelligence-collection purposes. The main differences between ASIO's security intelligence collection warrants, and the proposed criminal intelligence collection warrants for the AFP and ACIC, are:

- ASIO's computer access warrants are issued by the Attorney-General and authorise ASIO to collect intelligence that is relevant to 'security' within the meaning of that term in section 4 of the ASIO Act;[135] and
- the AFP and ACIC's network activity warrants would be issued by a judge or an AAT member, who has been appointed as an issuing authority in their personal capacity, and would authorise the AFP or ACIC (as applicable) to collect intelligence about a 'criminal network of individuals'.[136]

410. As discussed below, it is readily conceivable that there will be overlap between the intelligence collection activities of the AFP or ACIC and ASIO.

Similar attributes to the AFP and ACIC's existing computer access warrants

411. The issuing thresholds, issuing process and powers able to be authorised under network activity warrants are substantially similar to those applicable to the AFP and ACIC's computer access warrants.[137] The Bill also proposes that network activity warrants should be subject to an equivalent regime of mandatory assistance orders to those presently available in respect of computer access warrants under section 64 of the SDA. These orders can compel individuals with relevant knowledge or skills to render assistance to the AFP or ACIC in executing a warrant, or making intelligible data obtained under a warrant.[138]

412. These equivalencies means that many of the issues the Law Council has raised previously about aspects of the computer access warrant regime, and associated mandatory assistance orders, also apply to network activity warrants (in addition to data disruption warrants, as set out earlier in this submission).

Key differences to the AFP and ACIC's existing computer access warrants

413. The fundamental difference between the proposed network activity warrant regime and the existing computer access warrant regime is the purpose for which computer access and network exploitation activities may be carried out. That is, network activity warrants are issued for the purpose of collecting intelligence about a criminal

[135] ASIO Act, section 25A.

[136] Bill, Schedule 2, item 9 (especially proposed sections 27KK, 27KM, 27KN and 27KP of the SDA).

[137] Ibid, Schedule 2, item 9 (inserting proposed sections 27KK-27KP of the SDA).

[138] Ibid, Schedule 2, item 31 (inserting proposed subsection 64A(1) of the SDA).

network, or its individual members. Computer access warrants are issued for the purpose of collecting evidence about a suspected offence, as part of an investigation that is intended to lead to criminal law enforcement action.

414. There are three further differences apparent in the two warrant-based regimes:

- **evidential admissibility:** the Bill proposes that evidence obtained under a network activity warrant will be inadmissible in criminal proceedings, other than prosecutions of secrecy offences under the SDA for the unauthorised disclosure of 'protected information'. However, there is no prohibition on derivative use, and the Bill also proposes to expressly permit the use of information obtained under a network activity warrant in applications for other warrant types, such as computer access and data disruption warrants.[139] In contrast, information obtained under a surveillance device warrant or a computer access warrant is admissible evidence in a criminal proceeding;[140]

- **authorisation of the use of surveillance devices:** the Bill proposes that network activity warrants could authorise the use of a surveillance device for the purpose of doing any other thing authorised under the warrant—such as accessing data, or entering or existing premises—without requiring the issuance of a separate surveillance device warrant, or applying the same issuing threshold as for 'stand-alone' surveillance device warrants in existing Division 2 of Part 2 of the SDA.[141] This will be additional to a power to intercept telecommunications for the purpose of doing any other thing authorised under the network activity warrant. Presently, computer access warrants issued under Division 4 of Part 2 cannot authorise the use of surveillance devices, but since the enactment of the TOLA Act in 2018, may authorise the interception of telecommunications.[142] The same position applies to ASIO's computer access warrants;[143] and

- **oversight agency:** it is proposed that the IGIS, rather than the Ombudsman, will have oversight over the activities of the AFP and ACIC in exercising powers and performing functions under network activity warrants, on the basis that the IGIS should have comprehensive oversight over intrusive, warrant-based intelligence collection powers of agencies within the National Intelligence Community.[144] Two consequences of this are that:

  - the IGIS has broader functions than the Ombudsman, in that the IGIS may consider the propriety of agencies' activities (in addition to their legal compliance, compliance with applicable policies and human rights compatibility), as well as greater discretion about the timing and focus of inspections;[145] and

  - oversight responsibilities in relation to the AFP and ACIC's investigations of cyber-enabled crime will be fragmented where a single operation in relation to cyber-enabled crime is supported by multiple warrants or other orders, for example:

[139] Bill, Schedule 2, item 19 (inserting proposed subsections 45B(3), (5) and (10) of the SDA).

[140] SDA, subsection 45(5).

[141] Ibid, Schedule 2, item 9 (inserting proposed paragraphs 27KP(2)(i) and 27KP(8)(i) of the SDA).

[142] SDA, subsection 27E(2), especially paragraph (h) (telecommunications interception).

[143] ASIO Act, subsection 25A(4), especially paragraph 25A(4)(ba) (telecommunications interception powers).

[144] Bill, Schedule 2, item 23 (inserting proposed section 49D of the SDA) and Part 2 (especially items 51-90, which propose to amend the IGIS Act).

[145] IGIS Act, section 9A (inspections). See also, section 8 (intelligence agency inquiry functions).

- it may be possible to obtain one or more of a network activity warrant, a computer access warrant, a search warrant, an account takeover warrant, and a data disruption warrant;
- it may be possible to obtain compulsory assistance orders under the SDA, or Part 15 of the Telecommunications Act, to enable the AFP and ACIC to execute the above kinds of warrants, or to make intelligible data that has been obtained under those warrants; and
- depending on the nature and impacts of the relevant cyber-enabled crime under investigation, it could potentially trigger the mandatory intervention powers proposed in the Security Legislation Amendment (Critical Infrastructure) Bill 2020, which is separately under inquiry by the Committee.

Necessity of the regime

415. As an overarching comment on the proposed regime of network activity warrants, the Law Council queries the necessity of conferring warrant-based intelligence collection powers on the AFP and ACIC, both individually and cumulatively, in addition to their existing powers for the purpose of investigating suspected offences.

Necessity of specific, intrusive criminal intelligence-collection powers

416. The Law Council is concerned that the general policy objective outlined in the Explanatory Memorandum does not substantiate the necessity of the proposal to confer intrusive intelligence-collection powers on either the AFP and ACIC, both individually and collectively.

417. The Law Council acknowledges the difficulty identified in the Explanatory Memorandum in relation to the investigation of cyber-enabled crime, when suspects deliberately deploy anonymising technologies, or utilise other methods to obscure their identities and activities, particularly in their use of the 'dark web'.[146]

418. However, it does not follow from the mere existence of these investigative challenges that the legislative proposal to establish a specific, intrusive criminal intelligence-collection power is a necessary and proportionate response. The extrinsic materials to the Bill do not clearly address the reasons that the existing computer access warrant regime in Division 4 of Part 2 of the SDA is incapable of being utilised to effectively overcome the stated difficulties in identifying targets or suspects.

419. Proposals to confer significant new intrusive powers require compelling evidence that existing powers are inadequate. This is especially so when many of the existing powers available to the AFP and ACIC:

- have only been conferred recently;[147]
- are part of a suite of existing, extraordinary investigative powers;[148] and

[146] Explanatory Memorandum, 2 at [2]-[3] and 4 at [14]-[15].

[147] Computer access warrant powers were conferred by Schedule 2 to the TOLA Act, which was enacted in 2018. The Committee has not yet completed its first review of those powers.

[148] For example, surveillance device warrants, telecommunications interception warrants, computer access warrants, powers to compel assistance from the communications industry and others with knowledge of computers, controlled operations, the compulsory examination powers of the ACIC; and a number of specific measures in relation to terrorism offences, including: a lower arrest threshold; principal offences which specifically target merely preparatory conduct that is not covered by the inchoate offence of attempt; and specific post-arrest questioning powers.

- are additional to the ability of the AFP and ACIC to cooperate with intelligence agencies, including ASIO and ASD, which already have intrusive powers to access data held in, or accessible from, computers, specifically for intelligence gathering purposes.

Coverage of existing computer access warrant regime

420. The Explanatory Memorandum to the Bill focuses on investigative challenges in identifying targets or suspects in relation to cyber-enabled crime. However, it does not acknowledge that the computer access warrant regime in existing Division 4 of Part 2 of the SDA already contains measures to accommodate circumstances in which the identity of a suspect cannot be ascertained prior to the AFP or ACIC accessing data held in, or accessible from, a computer.

421. Presently, subsection 27A(1) of the SDA provides that a computer access warrant can be sought and issued if:

> *(a) one or more 'relevant offences' have been, are being, are about to be, or are likely to be committed;*
>
> *(b) an investigation into those offences is being, will be, or is about to be, or is likely to be conducted; and*
>
> *(c) access to data held in a computer (the target computer) is necessary, in the course of that investigation, to enable evidence to be obtained of:*
>
> *(i) the commission of those offences; or*
>
> ***(ii) the identity and location of the offenders*** (emphasis added).

422. Subsection 27A(15) also provides that computer access warrants can specify the 'target computer' in various ways. In particular, paragraph 27A(15)(c) provides that a target computer may be 'a computer that is associated with, used by, or likely to be used by' a person (whose identity may or may not be known)'. This makes explicit that the inability to conclusively establish the identity of a target will not preclude the issuance of a computer access warrant.

423. The Explanatory Memorandum does not provide insight into which one or more of these existing requirements have caused one or more of the following outcomes:

- operated to prevent the issuance of computer access warrants in connection with investigations of suspected cyber-enable crime;
- resulted in limitations in the scope of investigative powers; or
- otherwise unduly hindered the effective conduct of investigations.

Potential desire to reduce particularisation requirements for 'relevant offences'

424. The Law Council acknowledges that there may be a desire to effectively 'streamline' (by reducing) the authorisation requirements and process for computer access powers, where the full range of offending by members of a criminal network is unknown when an investigative warrant is first sought and issued.

Current requirements for computer access warrants

425. Presently the issuing threshold for a computer access warrant in subsection 27A(1) of the SDA, as extracted above, requires the particularisation of one or more 'relevant offences' that have occurred, are occurring, or are about to or are likely to

occur; and the commencement, or likely commencement, of an investigation into the 'relevant offence' or those 'relevant offences'. The intrusive powers authorised by a computer access warrant under section 27E are similarly limited to the purpose of gathering evidence in relation to the 'relevant offence' or 'relevant offences' specified in the warrant instrument.[149]

426. If further suspected 'relevant offences' are identified in the course of executing a computer access warrant, and those further offences are not covered by that warrant, it would presently be necessary for the AFP or ACIC to:

- if possible, seek a variation of the existing warrant to extend the 'relevant offences' covered; or
- seek a new warrant in relation to the additional 'relevant offences', which could be executed concurrently with the pre-existing warrant.

427. Each of these options would require the issuing authority to assess the warrant or variation request against the statutory issuing criteria in section 27C. (That is, the issuing authority must be satisfied that there are reasonable grounds for the suspicion founding the application; and must consider it appropriate to issue the warrant or variation, having regard to the nature and gravity of the 'relevant offence' or 'relevant offences'.)[150] Applications for an additional warrant, or a variation of an existing warrant, also generally need to be supported by an affidavit, which sets out the facts and grounds concerning the particular 'relevant offence' or 'relevant offences' that are the subject of the application.[151]

428. While the issuing thresholds for, and powers authorised under, computer access warrants are directed to evidence collection purposes in relation to one or more specified 'relevant offences', it is open to the AFP or ACIC to make secondary use of information obtained in the course of executing those warrants for intelligence purposes. For example, the AFP and ACIC may use information obtained from the warrant operation to build a picture of the nature, composition, activities, intentions, capabilities, *modus operandi*, funding sources and affiliations of a criminal enterprise or network of individuals. This work may be undertaken separately to, and concurrently with, enforcement action to enable the arrest, charge and prosecution of individual suspects.

Proposed requirements for network activity warrants

429. In contrast, if Schedule 2 to the Bill is passed, a network activity warrant would enable the issuance of a single warrant to authorise the collection of intelligence about the criminal network or its individual members, provided that this intelligence is assessed as being relevant to preventing, detecting or frustrating one of more **kinds** of 'relevant offences'.[152]

430. In other words, the issuing thresholds for network activity warrants, and powers authorised under those warrants, are not limited to the purpose of gathering evidence in relation to one or more specified 'relevant offences' which are suspected to have been committed, or are being committed, or are likely to be committed. This effective reduction in existing requirements of particularity in relation to 'relevant offences' would likely remove the need for multiple, simultaneous computer access warrants to be sought and issued; or the need for frequent variation of extant warrants as an investigation into a criminal network progresses. As a corollary, it

[149] SDA, subsections 27E(2) and 27E(4).

[150] Ibid, paragraphs 27C(1)(a) and 27C(2)(a) (issuing) and subsection 27F(3) (variation).

[151] Ibid, subsections 27A(8) and 27F(3).

[152] Bill, Schedule 2, item 9 (inserting proposed subsections 27KK(1)and 27KM(1) of the SDA).

also removes the existing requirements for independent authorisation, in relation to specific suspected 'relevant offences'.

431. New section 45B of the SDA effectively proposes a form of *quid pro quo* for broadening the scope of network activity warrants by removing particularisation requirements. Namely, it would limit the evidential admissibility of information obtained under those warrants in criminal and civil proceedings.[153]

432. However, information obtained under a network activity warrant could be utilised as the basis for requesting and issuing a computer access warrant (or another form of warrant, such as a surveillance device or search warrant), to authorise the collection of admissible evidence in relation to a 'relevant offence'. It could also be used as the basis for obtaining a data disruption warrant, or otherwise used derivatively in an investigation. For example, it could inform lines of questioning of suspects who are arrested on suspicion of an offence; or in an application for authorisation to conduct a controlled operation, and in the conduct of that operation.

The need for further information about perceived necessity

433. The extrinsic materials to the Bill do not explain why it is necessary to confer all of the powers under proposed section 27KP of the SDA at such a preliminary stage of an investigation, rather than the AFP or ACIC simply starting by obtaining a computer access warrant that particularised one or more 'relevant offences', and subsequently obtaining variations or additional warrants as further suspected 'relevant offences' are identified.

434. Given that the definition of a 'criminal network of individuals' in proposed section 7A of the SDA (for the purpose of the network activity warrant regime) requires proof that one or more individuals have engaged, are engaging, or are likely to engage in conduct that constitutes a 'relevant offence' or 'relevant offences', it would be legally possible to obtain an initial computer access warrant in connection with that offence or those offences.

435. The question is whether it is necessary for a single warrant (namely, a network activity warrant) to authorise the exercise of intrusive powers in connection with any other kind of suspected 'relevant offence' or 'relevant offences' that are assessed by the AFP or ACIC as being related to the identified criminal network, or any of its individual members. It should also be noted that the question of whether a particular suspected offence is of the same 'kind' or 'kinds' of relevant offences specified in the warrant instrument will be subject to unilateral determination by the AFP and ACIC, without external approval or review, prior to the exercise of intrusive powers.

436. Accordingly, it is incumbent on the proponents of this proposal to provide detailed and compelling justification of the necessity of effectively bypassing existing requirements for the external approval of intrusive powers, in relation to specific suspected offences. That justification must exceed the mere convenience or utility of such measures. As the Richardson Review commented in its unclassified report, it is important to rigorously test claims that existing statutory safeguards on intrusive powers should be removed because of their administrative impost on security or law enforcement agencies. As noted above, the Richardson Review cautioned that 'very often such claims do not withstand even modest inquiry' [154]

[153] Ibid, Schedule 2, item 19 (inserting proposed section 43B of the SDA).

[154] Richardson Review, *Unclassified Report, Volume 1* (December 2019), 34-35.

Duplication and overlap with intelligence agencies' functions

437. The Law Council also notes that there is significant potential for the intrusive powers under network activity warrants to overlap with the existing computer access and network exploitation powers of ASIO, where the activities of a criminal network under surveillance by the AFP or ACIC are also prejudicial to security. This reflects the fact that several 'relevant offences' within the meaning of section 6 of the SDA cover subject matter within the definition of 'security' in section 4 of the ASIO Act.

438. Overlap may be especially likely in relation to criminal networks who are suspected of engaging in, or facilitating, acts of foreign interference, terrorism or foreign incursions to commit hostile activities against the governments and people of other countries. These activities are covered by the definition of 'security' in section 4 of the ASIO Act, and also constitute offences against the security of the Commonwealth in Chapter 5 of the Criminal Code.[155] Accordingly, there is a risk of duplication, and potential oppression, as a result of a person being surveilled under multiple warrants issued to different agencies, in relation to the same or substantially similar activities.

439. Further, because the Bill proposes a regime for the extraterritorial application of network activity warrants,[156] there is also a realistic prospect of activities authorised under network activity warrants to overlap with the offshore activities of ASD in:

- collecting intelligence about the capabilities, intentions or activities of people or organisations outside Australia; or
- preventing or disrupting, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia.[157]

440. It should also be noted that the statutory functions of both ASIO and ASD include cooperation with Australian law enforcement agencies, both for the purpose of ASIO and ASD performing their functions, and for the purpose of law enforcement agencies performing their functions.[158]

441. The substantial risk that the highly intrusive powers conferred under network activity warrants may significantly duplicate or overlap with the existing powers of intelligence agencies casts doubt on the perceived necessity of conferring the AFP and ACIC with specific criminal intelligence-collection powers. The extrinsic materials to the Bill have not identified a clear gap in the availability of intrusive intelligence-collection powers available to emanations of the Commonwealth.

442. In addition to the existence of substantial doubt about the threshold question of the of the proposed network activity warrant regime, Schedule 2 to the Bill does not contain statutory safeguards to prevent and manage the risk of duplication, conflict and oppression to persons who may be subject to multiple, overlapping intrusive powers of ASIO, ASD, the AFP and ACIC. The Bill only proposes to require the AFP or ACIC to notify, and the issuing authority to consider, all network activity warrants that were previously sought or issued in relation to the criminal network.[159] However, it does not contain any statutory requirements for the AFP or ACIC, as applicant for a network activity warrant to:

---

[155] Criminal Code, Parts 5.2 (espionage and foreign interference), 5.3 (terrorism) and 5.5 (foreign incursions).

[156] Bill, Schedule 2, item 11 (inserting proposed section 43E of the SDA).

[157] *Intelligence Services Act 2001* (Cth) (**ISA**), paragraphs 7(1)(a) and (c).

[158] ISA, paragraph 7(1)(f) and sections 13 and 13A; and ASIO Act, sections 19 and 19A.

[159] Bill, Schedule 2, item 2 (inserting paragraph 27KM(2)(g) of the SDA).

- inform the issuing authority as to whether the target is, or has previously been, the subject of intrusive powers of surveillance by any other agency in respect of the same, or substantially similar, activities; and
- if the target is the subject of concurrent surveillance, or has previously been the subject of surveillance, by another agency, demonstrate the necessity and proportionality of the network activity warrant being sought.

443. The absence of requirements for the issuing authority to be routinely informed of, and consider, all concurrent or previous intrusive surveillance deployed against a target (or another person whose data may be accessed) undermines the accuracy of the proportionality assessment that the issuing authority is required to perform, in determining whether to issue a network activity warrant.[160]

Necessity of conferring powers on both the AFP and ACIC

444. If the Committee is persuaded that it is necessary to confer a specific computer access power for criminal intelligence purposes, as distinct to the collection of evidence to enable the enforcement of offences, the Law Council questions whether it is necessary for such a power to be conferred on **both** the AFP and the ACIC, rather than the ACIC alone as the specialist national criminal intelligence agency.

445. The extrinsic materials to the Bill do not provide any explanation of the proposal to confer warrant-based intelligence collection powers on both the AFP and the ACIC. Nor do the provisions of Schedule 2 to the Bill provide any guidance about the following matters:

- the circumstances in which it is intended that either the AFP, or alternatively the ACIC, would be responsible for the collection of criminal intelligence under a network activity warrant; and
- the mechanisms in place or in preparation for avoiding duplication or conflict between the intelligence collection activities of the AFP and ACIC; and
- the mechanisms by which the issuing authority considering a warrant application by one agency (for example, the ACIC) will be informed of previous or extant warrants or applications made by the other agency (for example, the AFP) which cover the same ground as the application under consideration.

446. The Law Council acknowledges that both the AFP and the ACIC perform criminal intelligence functions. However, it does not follow automatically from the existence of these functions that both of these agencies require specific, intrusive intelligence collection powers, which effectively dilute the existing requirements of particularisation under computer access warrants in Division 4 of Part 2 of the SDA.

447. The Law Council further notes that limiting network activity warrants to the ACIC, as the specialist federal criminal intelligence agency, could provide a stronger degree of assurance about the use of these powers. That is, the ACIC would utilise these powers, along with its other warrant-based powers, as part of its special investigations or operations. These operations require prior approval from the ACIC's governing board.[161] The membership of that board includes the AFP Commissioner (who is the Chair), as well as State and Territory Police Commissioners, the Director-General of Security, the Secretary of the Department of Home Affairs and the Comptroller-General of Customs (the Australian Border Force

[160] Ibid, Schedule 2, item 9 (inserting paragraphs 27KM(2)(d)-(g) of the SDA).

[161] *Australian Crime Commission Act 2002* (Cth) (**ACC Act**), paragraphs 7C(1)(c) and (d) and subsections 7C(2) and (3).

Commissioner).[162] Moreover, it would be possible for AFP members to be made available to the ACIC for particular operations.[163]

Law Council recommendations on the threshold question of necessity

448. In view of the above matters, the Law Council considers that the proposed network activity warrant regime should not proceed, unless and until a detailed and compelling justification is provided of the necessity of the following proposals:

- creating a 'stand-alone' regime of intrusive computer access powers for criminal intelligence collection purposes, as distinct to the continued utilisation of computer access warrants under Division 4 of Part 2 of the SDA; and
- conferring powers to seek and execute network activity warrants on both the AFP and ACIC, rather than the ACIC alone as the national specialist criminal intelligence body.

449. An adequate justification of the necessity of the network activity warrant regime would need to extend beyond a general reference to operational challenges under existing warrant-based computer access powers. This is presently the extent of the justification provided in the Explanatory Memorandum.

Key scrutiny issues

450. If the Committee considers that there is a compelling justification for one or both of the AFP and ACIC to have warrant-based computer access powers for criminal intelligence purposes, the Law Council encourages the Committee to consider the issues outlined in this submission, concerning the scope of the proposed powers and the design of the warrant-based authorisation framework. In particular:

- equivalent issues to those outlined above in relation to data disruption warrants, and associated mandatory assistance orders, including:
  - the appropriate issuing authority, having regard to matters of independence and expertise;
  - the breadth of powers to intercept telecommunications, use force against persons and things, and temporarily remove computers and other things from premises entered under the warrant;
  - limitations in reporting and record-keeping requirements;
  - inadequacies in secrecy provisions, which do not enable the disclosure of 'protected information' (essentially, information about the existence of a warrant or information obtained under a warrant) for the purpose of obtaining legal advice; and
  - significant issues in relation to mandatory assistance orders, including:
    - an absence of statutory requirements for all mandatory assistance orders to contain certain key particulars;
    - an absence of reporting requirements in relation to mandatory assistance orders issued alongside warrants; and
    - replication of problematic provisions identified by the third INSLM in his review of the TOLA Act, which considered mandatory

[162] Ibid, subsections 7B(2) and (3).

[163] Ibid, paragraph 49(a). See also, section 4 (definition of a 'member of staff of the ACC' especially paragraph (e) in relation to members of the AFP who are made available under section 49).

assistance orders in relation to data accessed under computer access and search warrants;

- the proportionality of the proposed powers, with respect to:
  - the persons who may be targeted (including the breadth of the definition of 'criminal network of individuals' and the component term 'electronically linked group of individuals');
  - the application of the warrant regime to 'relevant offences' within the meaning of section 6 of the SDA; and
  - the power to use surveillance devices, without requiring separate authorisation under a surveillance device warrant; and
- issues concerning overlap of, and possible inconsistency with, the collection powers of intelligence agencies, particularly ASIO and ASD, including:
  - the absence of any requirement for the issuing authority to be informed of, and consider, the combined impacts of multiple intrusive intelligence collection powers on the target or others (for example, ASIO computer access warrants, or other surveillance powers of ASIO, ASD, ACIC or the AFP); and
  - the appropriateness of the proposed provisions enabling the extraterritorial operation of network activity warrants, in view of ASD's powers in relation to persons outside Australia; and
  - the creation of a disjunct between the issuing criteria for the AFP and ACIC's network activity warrants, and ASIO's computer access warrants for security intelligence purposes. In particular, despite both forms of warrants authorising near identical activities for criminal intelligence collection warrants:
    - only network activity warrants will be subject to external authorisation (with ASIO's warrants issued by the Attorney-General); and
    - the statutory issuing criteria for ASIO's warrants (which have the effect of placing legal limitations on the issuing power of the Attorney-General, and therefore the validity of warrants) do not require an assessment of proportionality, including third-party impacts.[164] Network activity warrants include issuing criteria directed explicitly to these matters.[165] In the case of ASIO, proportionality is only the subject to general guidance in administratively binding guidelines, breach of which has no impact on the legal validity of its intrusive powers.[166]

Common issues with computer access warrants and data disruption warrants

451. The proposed network activity warrant regime raises the following, equivalent issues to those discussed above for data disruption warrants:

[164] ASIO Act, subsection 25A(2).

[165] Bill, Schedule 2, item 9 (inserting proposed paragraphs 27KC(1)(b) and 27KC(2)(a)-(d) of the SDA).

[166] The Hon Peter Dutton MP, *Minister's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its functions and the exercise of its powers*, (August 2020), 11-12 at [3.4]-[3.6] (**ASIO Guidelines**). The ASIO Guidelines are made under section 8A of the ASIO Act.

- overbreadth in the concept of a ‘relevant offence’ in section 6 of the SDA for the purpose of intrusive intelligence collection powers, which will enable such warrants to be issued with respect to a wide range of offences, including:
    - offences which are far removed from the stated purpose of the Bill to target serious and organised crime, and in fact capture conduct at the lower end of the range of objective seriousness;
    - an unlimited range of further offences that may be prescribed by regulation, irrespective of their nature or maximum penalty; and
    - a wide range of State and Territory offences, which fall within the definition of a ‘State offence that has a Federal aspect’ in section 7 of the SDA (which is component of the term ‘relevant offence in section 6), because they could have been the subject of Commonwealth laws, had the Commonwealth elected to exercise its legislative power in that area;
- incomplete statutory requirements for the assessment by the issuing authority of the necessity and proportionality of the proposed warrant;
- the ability of the Attorney-General to appoint AAT members as issuing authorities for warrants, rather than superior court judges alone;
- overbreadth in the powers that may, or must, be authorised under a warrant, including:
    - issues relating to telecommunications interception, including overbreadth in the purpose for which interception can be undertaken, low thresholds for exercising interception powers, and overbreadth in powers to make subsequent use and disclosure of intercept information;
    - overbreadth in the purposes for which force may be used against persons or things under a warrant; and
    - inadequate statutory safeguards and ambiguities in the scope of powers to temporarily remove computers and other things from premises;
- issues pertaining to the potential involvement of ASD in the regime, including:
    - overlap between the proposals in Schedule 2 to the Bill to enable the extraterritorial execution of network activity warrants, and ASD’s existing intelligence collection and cybercrime disruption functions under the ISA; and
    - a lack of clarity about the legal basis upon which ASD staff members may assist the AFP and ACIC in executing network activity warrants (that is, as secondees to the AFP or ACIC, or as part of ASD’s cooperation function in paragraph 7(1)(f) and section 13A of the ISA);
- numerous issues in relation to mandatory assistance orders, including:
    - a lack of demonstrated necessity for the proposed power;
    - overbreadth in the persons whose assistance may be compelled;
    - low issuing thresholds that do not require a comprehensive assessment of necessity and proportionality;
    - absence of any statutory requirements for orders to specify key particulars;
    - non-implementation of recommendations of the third INSLM in relation to existing forms of mandatory assistance orders; and

- limitations in oversight, primarily an absence of reporting and record-keeping requirements, which are equivalent to the requirements for the underlying warrant under which computer access is authorised;

- issues pertaining to emergency authorisations with respect to network activity warrants, especially:
  - an absence of demonstrated necessity for urgent intelligence collection powers, as distinct to enforcement powers; and
  - overbreadth in the classes of authorising officer from the ACIC; and
- potentially arbitrary impacts of the existing secrecy provisions of the SDA in relation to protected information, which may prevent disclosures of the existence of network activity warrants, or action taken under the purported authority of such warrants, for the purpose of obtaining legal advice.

452. Accordingly, the Law Council's recommendations 3, 5-7, 10, 11-13, 15-19, 24, 28-33 in relation to data disruption warrants apply equally to network activity warrants.

Recommendation 36—common issues with other warrant types

- **The Law Council's recommendations 3, 5-7, 10, 11-13, 15-19, 24, 28-33 in relation to the proposed data disruption warrant regime should also be implemented with respect to equivalent provisions in the proposed network activity warrant regime.**

Definition of a 'criminal network of individuals'

453. In addition to the abovementioned matters concerning the proposal to link the new warrant-based power to the concept of a 'relevant offence', the Law Council considers that the proposed definition of a 'criminal network of individuals' and its component term 'electronically linked group of individuals' is overly broad.

454. Proposed section 7A of the SDA sets a low threshold for the definition of a 'criminal network of individuals'. It only requires the existence of a group of individuals who are using the same electronic service, or communicating with each other using an electronic service, and for a minimum of one of those individuals to have engaged or facilitated, be engaging or facilitating, or be likely to engage in or facilitate, a 'relevant offence'.

No requirement to establish a nexus between the suspected actions of an individual group member, and the suspected actions or intentions of the group as a whole

455. There is no requirement for the overall group to be working in pursuit of a common criminal purpose, in order to be deemed a 'criminal network' under proposed section 7A. Nor are there any other unequivocal statutory requirements for the suspected 'relevant offence' to have been committed or facilitated in connection with the individual's membership of the group. In fact, there is no requirement for members of the group to even know, or have reasonable grounds to suspect, that another individual member has committed or facilitated the commission of a 'relevant offence', or is doing so, or is likely to do so.

456. It also appears that the concept of a 'criminal network of individuals' could cover a group of people who are passively engaging with the same electronic service without actually communicating with each other, or any member of the group who is involved in the commission of a relevant offence. (For example, people who are members of the same online discussion forum or social media platform.)

457. The lack of a clear statutory requirement to establish a nexus between an individual group member's recent, current or anticipated offending, or facilitation of offending, and their involvement in the group, creates a risk that legitimate groups may be targeted under network activity warrants. That is, a group may be organised for lawful and legitimate purposes, such as protest or advocacy and may use electronic communications, such as email or social media, to organise and conduct its affairs. If at least one individual person who participated in those communications has also separately engaged in, or facilitated, the commission of a relevant offence, the entire group would be covered by the statutory definition of a 'criminal network of individuals' for the purpose of the network activity warrant regime.

458. Under proposed subsection 27KK(1) of the SDA, a network activity warrant would enable the AFP or ACIC to access to any computer used, or likely to be used, by **any member** of the group (as the 'target computer').

459. This is compounded by the broad scope of a 'relevant offence' as discussed previously in this submission. It means that there need only be a suspicion that an individual member has committed or facilitated the commission of any offence punishable by three or more years' imprisonment, or is doing so, or is likely to do so (or alternatively, an offence prescribed by regulations; or a State or Territory offence that the Commonwealth Parliament has concurrent legislative power to enact).

460. The Law Council acknowledges that proposed paragraph 27KK(1)(b) of the SDA attempts to impose some additional requirements, which are directed to an assessment of the anticipated intelligence value of any information obtained from accessing data held in the target computer. Namely, access to that data must be assessed as being likely to substantially assist in the collection of intelligence that:

    (i) *relates to the group **or** to any of the individuals in the group* [emphasis added]*; and*

    (ii) *is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.*

461. However, this further criterion does not overcome the risks of overbreadth arising from the lack of a statutory requirement for proof of a nexus between the conduct of an individual group member or members, and the nature and activities of the group as whole. Rather, subparagraph (i) makes explicit that the intelligence need only relate to any individual in the group. It is not essential that the intelligence relates to the actions or intentions of the group as a whole.

462. Subparagraph (ii) also covers a wide range of offences. Not only does it incorporate the concept of the commission of a 'relevant offence' by any person, but it also applies the concept of a 'kind' of relevant offence.

463. As noted above, in relation to similar provisions in the proposed data disruption warrant regime, the task of assessing whether a particular suspected 'relevant offence' is of the same 'kind' of 'relevant offences' specified in a warrant is likely to be complex and potentially subjective. The decision-making of the relevant AFP or ACIC officers executing a warrant will not be subject to independent approval prior to the exercise of powers in reliance on that decision.

Anticipatory nature of intelligence collection activities

464. It is also important to recognise that the question of whether intelligence is 'relevant' to a matter, such as the prevention, disruption or frustration of a kind of 'relevant offence', will be informed by the necessarily anticipatory nature of intelligence-

collection activities. Such an interpretation is likely to further expand the scope of intelligence collection powers capable of being authorised under the proposed network activity warrant regime, and therefore further exacerbate the risk of overbreadth.

465. By way of analogy, in relation to the construction of a similar provision in the ASIO Act, concerning the meaning of the expression 'intelligence relevant to security' for the purpose of ASIO's functions, the High Court has held that such intelligence would be relevant 'if it can reasonably be considered to have a reasonable connection with that topic, judged in light of what is known to ASIO at the relevant time'.[167] The High Court held that the concept of the 'relevance' of intelligence to the purpose of security under the ASIO Act could cover the collection by ASIO of intelligence to determine **whether** a person is a security risk, provided that ASIO is acting on initial information which suggests a possibility the person may be such a risk. In other words, provided that the initial information is not self-evidently lacking in credibility, it may permissibly be 'checked out and followed up'.[168]

466. A similar, purposive construction of the concept of 'intelligence relevant to the prevention, detection or frustration' of a relevant offence in proposed section 27KK of the SDA could also mean that a network activity warrant may be sought and issued on the basis of preliminary, and fairly minimal, information suggesting a possibility a relevant offence that could be prevented, detected or frustrated, in order to **either** confirm or exclude that possibility.

467. The Law Council therefore recommends that proposed section 27KK of the SDA (item 9 of Schedule 1 to the Bill) should be amended to expressly require proof of a reasonable suspicion of a nexus between the activities of an individual member of a group; and the activities, purpose or intentions of the group as a whole. This should be implemented via amendments to the definition of a 'criminal network of individuals' in proposed section 7A of the SDA.

Recommendation 37—definition of a 'criminal network of individuals'

- **The following amendments should be made to Schedule 2 to the Bill:**
  - **The definition of a 'criminal network of individuals' in proposed section 7A of the SDA (item 8 of Schedule 1 to the Bill) should be amended to require there to be a reasonable suspicion of a nexus between:**
    - **the suspected conduct of an individual group member in committing an offence, or facilitating the commission of an offence (or having done so, or being likely to do so); and**
    - **the actions or intentions of the group as a whole.**

    (That is, there should be a requirement to establish that the group as a whole was pursuing a common criminal purpose, and the conduct of the individual member or members was directed to that common criminal purpose.)
  - **The requirements in proposed paragraph 27KK(1)(b) (item 9 of Schedule 2 to the Bill) should also be amended to require proof that access to data held in the target computer is likely to**

[167] *Church of Scientology v Woodward* (1982) 154 CLR 25 at 61 (per Mason J).
[168] Ibid.

substantially assist in the collection of intelligence that:

- **relates to the group, or the actions of one or more of its individual members <u>in pursuit of a common criminal purpose of the group</u>; and**
- **is relevant to the prevention, detection or frustration of one or more kinds of relevant offences, <u>which are committed or facilitated in pursuit of a common criminal purpose of the group (or are likely to be so committed or facilitated).</u>**

Power to use surveillance devices without a separate warrant

468. Proposed paragraph 27KP(2)(i) provides that a network activity warrant may authorise the AFP or ACIC to use a surveillance device to do any act or thing specified in the warrant (for example, entering or exiting premises, using the target computer to obtain access to relevant data, or intercepting a telecommunication). As noted above, this power has no equivalent in the existing provisions governing computer access warrants in the SDA or ASIO Act.

469. The Explanatory Memorandum to the Bill states that the power to use a surveillance device under a network activity warrant is considered necessary to enable the execution of that warrant (for example, using an optical surveillance device for the purpose of being able to enter premises covertly).[169] It states that the existing thresholds for 'stand-alone' surveillance device warrants under Division 2 of Part 2 of the SDA may not always extend to the use of surveillance devices for this purpose, as they are directed to the investigation of an offence.[170]

470. Apart from the isolated hypothetical example noted above, the Explanatory Memorandum does not provide justification for the proposal to enable network activity warrants to authorise the use of a surveillance device, of any kind, for the purpose of doing any of the wide range of acts or things that may, or must, be authorised under such a warrant. The Explanatory Memorandum also does not justify why the perceived need to utilise surveillance devices to enable the covert execution of warrants cannot be fulfilled through other means, including performing physical surveillance of premises or using surveillance devices in circumstances in which a warrant is not required.

471. The Law Council is also concerned by the evident trend, which began with the TOLA Act in 2018, towards enabling warrants that authorise access to computer-based data (such as computer access and network activity warrants) to also authorise additional forms of electronic surveillance that have, until now, required authorisation under a separate warrant. The TOLA Act effected this change in relation to telecommunications interception powers under computer access warrants, so that a computer access warrant is now capable of authorising the interception of telecommunications for the purpose of doing any other act or thing that is authorised under the warrant (such as accessing data, or entering or exiting premises).[171]

472. The Bill now proposes to extend this 'incidental' use of intrusive electronic surveillance in relation to network activity warrants, by also conferring a power to use surveillance devices for the purpose of doing any act or thing authorised under a network activity warrant. The Law Council cautions that this apparent trend

[169] Explanatory Memorandum, 80 at [386].
[170] Ibid at [387].
[171] SDA, paragraph 27E(2)(h) (telecommunications interception under computer access warrants).

appears to undermine the intent of the Richardson Review, which specifically recommended against the establishment of a single electronic surveillance warrant, which is capable of authorising multiple, or all, forms of electronic surveillance.

473. The Law Council acknowledges that, under the network activity warrant regime, the purpose for which a surveillance device may be used is more limited than under a stand-alone surveillance device warrant. (That is, the surveillance device must be used only for the purpose of doing any other act or thing authorised under the warrant, rather than directly collecting intelligence about a criminal network, or evidence of a relevant offence.) However, this more limited purpose is likely to be largely neutralised by three factors:

- the breadth and diversity of the acts and things that can be authorised under a network activity warrant pursuant to proposed section 27KP of the SDA.[172] This is exacerbated by the broad definition of 'computer' in section 6 of the SDA, which is capable of covering a large number of individual devices, such as those connected to one or more networks;[173]
- the breadth of persons who may be the target or surveillance, given the breadth of the definition of 'computer' in the SDA, and the breadth of the proposed definition of a 'criminal network of individuals'; and
- the broad ability under proposed section 45B of the SDA to disclose and make secondary use of information obtained from the use of material obtained from the use of surveillance device pursuant to a network activity warrant (such as video footage or audio recordings). This includes:
  - the ability to use the surveillance material for the purpose of the AFP or ACIC obtaining another form of warrant for evidence collection or data disruption purposes;[174]
  - the ability to share the surveillance material with intelligence agencies for the purpose of those agencies performing any of their functions;[175]
  - the ability to share the surveillance material with other law enforcement agencies, such as State and Territory police;[176] and
  - the ability to use the surveillance material in civil proceedings, which could include applications for control orders or criminal confiscation orders.[177]

Dilution of particularisation requirements

474. The provisions of Schedule 2 to the Bill do not contain statutory criteria to limit the specific acts or things in respect of which a surveillance device can be authorised (such as covertly entering or exiting premises only, to the exclusion of all other acts or things authorised under the warrant). Nor is there any statutory requirement for all warrant applications to particularise the specific type or types of surveillance

[172] Bill, Schedule 2, item 9 (inserting proposed subsection 27KP(2) of the SDA). This ranges from entering and exiting premises, to accessing data that is held or is accessible from a computer, intercepting telecommunications, removing a computer or thing from premises and returning it, and concealing that any act or thing was done under the warrant.

[173] SDA, section 6 (a computer is defined to mean: one or more individual devices; one or more computer systems; one or more computer networks; or any combination of the above).

[174] Bill, Schedule 2, item 19 (inserting proposed paragraph 45B(5)(d) of the SDA).

[175] Ibid (inserting proposed paragraphs 45B(4)(d) and (e) of the SDA).

[176] Ibid (inserting proposed paragraph 45B(11) of the SDA).

[177] Ibid (inserting proposed paragraph 45B(10)(b) of the SDA).

sought to be used (for, example, an optical surveillance device only). Unless an individual issuing authority decided to exercise their discretion to impose such conditions on an individual network activity warrant, these matters would be left to the discretion of the AFP and ACIC members responsible for executing the warrant.

475. It is important to note that the statutory definition of a 'surveillance device' in existing section 6 of the SDA covers a diverse range of devices (being data surveillance, optical surveillance, listening and tracking devices, a single device which combines two or more of these surveillance functions, and any other kind of device prescribed by regulation).

476. In contrast, the statutory requirements governing applications for surveillance device warrants require the AFP and ACIC to particularise the form of surveillance sought to be authorised.[178] Consequently, the issuing authority for a surveillance device warrant is required to assess the necessity and proportionality of the specific forms of electronic surveillance proposed to be carried out. If the AFP or ACIC subsequently sought to deploy additional types of surveillance capabilities in an investigation, which were not authorised under an extant surveillance device warrant, then it would be necessary for those agencies to obtain a variation to the extant warrant, or obtain a further warrant.

477. The proposal to dilute these particularisation requirements in relation to the authorisation of surveillance devices under network activity warrants means that:

- if a network activity warrant was issued on the basis of an application which identified the need to conduct optical surveillance of persons entering and exiting premises; but
- the network activity warrant instrument did not specify that only this type of surveillance device could be used, for this purpose alone (but rather reproduced in full the text of proposed paragraph 27KP(2)(i) of the SDA); then
- it would be lawful for the AFP or ACIC to also do the following activities (for example), at their discretion during the warrant operation, without any need for specific external authorisation from an issuing authority:
  - use a data surveillance device to assist them in gaining access to relevant data held in or accessible from a computer (for example, monitoring a person who is using a computer to isolate their particular activities on a computer system or network); or
  - use a listening device or tracking device for the purpose of determining whether it would be feasible to temporarily remove a computer or other thing from premises, or return the item covertly. (For example, to determine the movements of people who are known to visit, or are likely to visit, the premises, to ensure that the activities are conducted when the premises are vacant.)

478. Accordingly, the proposed power to use surveillance devices under network activity warrants represents a significant dilution of the existing requirements for the particularisation of the desired form of surveillance. As a result, the proposed conferral of powers to use surveillance devices under network activity warrants will effectively devolve approval requirements for the specific type of surveillance from the issuing authority (as is currently the case for surveillance device warrants) to the AFP or ACIC officers responsible for the execution of a network activity warrant.

[178] SDA, subparagraphs 14(5)(a)(ii) and 17(1)(b)(v).

Impact on mandatory 'use of force' authorisation

479. Proposed paragraph 27KP(7)(a) of the SDA provides that all network activity warrants must authorise the use of any force against persons and things that is necessary and reasonable to do any of the things specified in the warrant. This means that all network activity warrants must authorise the use of force for the purpose of using a surveillance device under the warrant.

480. The Explanatory Memorandum does not acknowledge or justify this extension of the power to use force, which limits the right to liberty and security of the person. In the absence of justification, particularly in the context of the large number of individuals against whom force could potentially be used due to the breadth of the scope of network activity warrants, the Law Council considers that it should not proceed.

The need for more specific statutory approval requirements

481. The Law Council is also concerned by the practical possibility that applications for network activity warrants could, as a matter of routine, seek authorisation of all of the discretionary powers listed in proposed subsection 27KP(2), including the use of surveillance devices to do any act or thing authorised under the warrant. In the result, the warrant application and warrant instrument (if ultimately issued) would simply repeat the text of proposed subsection 27KP(2). Such a practice creates a practical risk that there may be inadequate scrutiny of requests for authorisation to use a surveillance device under a network activity warrant.

482. In this regard, the Law Council notes that the AAT has previously provided information to the Parliament, which identified instances of AAT members spending highly condensed periods of time in considering applications for existing types of electronic surveillance warrants.[179] The Law Council has also previously given evidence to the Committee, which expressed concern that the reported timeframes did not, as a general observation, appear to be conducive to the detailed scrutiny of complex technical, factual and legal matters involved in determining requests for authorisation to exercise intrusive powers.[180]

483. Given that applications for network activity warrants will be made and determined covertly in circumstances in which time is likely to be of the essence, it is important that there are clear statutory safeguards (as recommended below) to prevent this risk from arising.

484. This will also ensure that the Parliament and the public have a credible basis upon which to be assured that all warrant requests seeking authorisation to use a surveillance device will routinely be scrutinised in detail, in relation to the specific form or forms of surveillance and the specific purposes of that surveillance.

485. Such statutory safeguards would ideally operate in combination with the Law Council's earlier recommendations for issuing authorities to be limited to superior court judges appointed in their personal capacities. If that recommendation is not implemented, there would be a heightened need for more detailed statutory

---

[179] Administrative Appeals Tribunal, *LCC-SBE19-203—Warrants under the Surveillance Devices Act 2004 Issued by the AAT*, Response to Question on Notice, Budget Estimates 2019-20, Senate Legal and Constitutional Affairs Committee, (22 October 2019), 5 (questioner: Senator the Hon K Carr). This evidence states: 'The average (mean) length of all appointments held since 1 July 2015, for any purpose, that are recorded as relating to an application under this Act [the SDA] is 24 minutes. The shortest amount of time recorded for an appointment that proceeded is 1 minute'.

[180] Dr D Neal SC, Law Council of Australia, *Committee Hansard, PJCIS*, Canberra, 12 May 2020, 14-15 (questioner: Hon M Dreyfus QC MP).

approval requirements for any use of surveillance devices under the authority of a network activity warrant.

Recommendation 38—power to authorise the use of surveillance devices

Preferred option

- **The Bill should be amended to omit the power to use surveillance devices under a network activity warrant, in proposed paragraph 27KP(2)(i) of the SDA (item 9 of Schedule 2 to the Bill).**
- **The corresponding concealment power in proposed paragraph 27KP(8)(i) should also be omitted.**

Alternative (non-preferred) option

- **If network activity warrants are to be capable of authorising the use of a surveillance device, proposed paragraph 27KP(2)(i) should be amended so that the issuing authority is required to specifically approve the following matters:**
  - **the activities under proposed section 27KP(2) for which a surveillance device may be used; and**
  - **the specific type or types surveillance devices that may be used for those activities.**
- **The power to use surveillance devices for the purposes of concealment under proposed paragraph 27KP(8)(i) should be similarly limited to the activities and purposes that were approved under proposed paragraph 27KP(2)(i).**

Oversight arrangements

486. The amendments in Part 2 to Schedule 2 to the Bill propose to confer oversight functions on the IGIS in relation to the ACIC and AFP's activities in:

- collecting, correlating, analysing, producing and disseminating intelligence obtained from the execution of network activity warrants; and
- performing functions or powers under a network activity warrant, or any other provision of the SDA that relates to network activity warrants. (Importantly, this will include the execution of mandatory assistance orders in relation to network activity warrants.)[181]

487. The Law Council has commented substantively on the proposed arrangements for IGIS oversight over network activity warrants in its separate submission to the Committee on the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (**IM Bill**), which includes them as contingent amendments.

488. It should also be noted that the IM Bill will expand the IGIS's oversight over the ACIC to all of that agency's activities that involve the collection, correlation, analysis, production and dissemination of intelligence, and not merely under network activity

[181] Bill, Schedule 2, item 55 (amending subsection 3(1) of the IGIS Act to insert a definition of 'intelligence function' of the AFP and ACIC). See also item 56 (inserting new subsection 8(3A) of the IGIS Act, conferring oversight functions on the IGIS in relation to the intelligence functions of the AFP and ACIC).

warrants.[182] However, the functions of the IGIS in relation to the AFP would be limited to oversight of network activity warrants alone. The Ombudsman would be responsible for oversight of the remainder of the AFP's activities.

489. As noted in its submission on the IM Bill, the Law Council is supportive of the proposal for the IGIS to have oversight responsibilities for these powers, given their focus on intelligence collection. The Law Council also supports the proposed amendments to enable information sharing between the IGIS, Ombudsman and other Commonwealth integrity agencies with relevant oversight responsibilities for the ACIC and AFP, including the Australian Information Commissioner and the Australian Human Rights Commission.[183]

490. The Law Council notes two issues that the Committee may wish to consider in relation to the scope of oversight over the new powers:

- **fragmentation of oversight—**there is a risk that oversight may become fragmented in relation to investigations by the ACIC and AFP into cyber-enabled crimes that are supported by multiple, individual warrants of different types, some of which are within IGIS oversight (in the case of network activity warrants) and the remainder of which are within the remit of Ombudsman oversight (such as computer access, data disruption and account takeover warrants). In these instances, differences in the nature of the oversight functions and powers of the IGIS and Ombudsman may result in 'lopsided' oversight. For example:

  - only the IGIS, not the Ombudsman, has a function to conduct oversight of the propriety of an agency's activities (whereas the functions of the Ombudsman are focused on legal compliance and administrative best practice);[184] and

  - the inspection functions of the Ombudsman are less flexible than those of the IGIS. The Ombudsman is required to inspect agencies' records at prescribed intervals for the purpose of assessing their compliance with legislative requirements (although it would be open to the Ombudsman to decide to conduct more frequent inspections). In contrast, the inspection functions of the IGIS can be performed at times and frequencies determined by the IGIS, and focus on the specific matters of legality and propriety that are determined by the IGIS for the particular inspection;[185] and

- **resourcing**—it will be important to ensure that the IGIS has sufficient resources to perform oversight of network activity warrants, without any reduction in existing levels of oversight over the six agencies presently within its remit. While the IGIS has received significant budgetary increases from 2017-18, the former Inspector-General has given evidence to the Committee that these resources have been applied to conduct oversight of expansions to

[182] IM Bill, Schedule 2, item 60 (amending subsection 3(1) of the IGIS Act to insert a new definition of 'intelligence function' in relation to ACIC) and item 61 (inserting new subsection 8(3A) of the IGIS Act to expand the 'intelligence agency inquiry' functions of the IGIS in relation to the ACIC beyond network activity warrants, to all of its activities that involve the collection, correlation, analysis, production and dissemination of intelligence for the purpose of performing its statutory functions).

[183] See especially: Bill, Schedule 2, item 71 (inserting new Part IIIA of the IGIS Act).

[184] See, for example: SDA, subsections 55(1) and (2) (inspection functions in relation to the SDA). See further: Ombudsman, *Submission to the PJCIS Review of the Surveillance Legislation Amendment (Data Disruption) Bill 2020*, (February 2021), 2 at [12] (comparative table).

[185] SDA section 55. Cf IGIS Act, section 9A.

ASIO powers conferred by the TOLA Act.[186] Further, both the IGIS and the Richardson Review have flagged the need for the IGIS to have access to independent technical expertise to conduct effective oversight, which will have resource implications.[187] It is not clear that such costs could be met from the existing budget of the IGIS, without a reduction in existing levels of oversight.

491. The Law Council therefore recommends that further consideration is given to these budgetary matters, as well as options to ensure consistent and comprehensive oversight of AFP operations in relation to cyber-enabled crime that are supported by multiple warrant types. (These matters are further elaborated in the Law Council's separate submission on the IM Bill dated 4 March 2021.)

Recommendation 39—oversight of network activity warrants

- **The Government should ensure that the budget of the IGIS is increased as necessary to ensure that there is no reduction in current levels of oversight as a result of the expansion of its functions, including in relation to network activity warrants.**
- **Further consideration should be given to mechanisms to ensure that a single operation by the AFP into cyber-enabled crime is subject to consistent and comprehensive oversight, irrespective of the particular oversight body responsible for different warrant types. In particular, consideration should be given to:**
  - **revising the proposal to only invest the IGIS with oversight functions in relation to the AFP under network activity warrants, and to expand oversight functions to cover all of the AFP's activities that involve the collection, correlation, analysis, production or dissemination of intelligence; or**
  - **expanding the inspection functions of the Ombudsman to include matters of propriety, and to have a similar degree of flexibility in relation to timing and focus as the inspection functions of the IGIS.**

Broader implications for ASIO's computer access warrants

492. The proposal to establish the network activity warrant regime for the AFP and ACIC would mean that ASIO is no longer the sole Commonwealth agency permitted, under warrant, to access computer-related data that is located inside Australia, for the purpose of collecting intelligence.

493. A broader consequence of enacting the network activity warrant regime is that there would be two sources of warrant-based, domestic computer access powers for intelligence collection purposes—one under the SDA (network activity warrants for the AFP and ACIC) and the other under the ASIO Act (computer access warrants for ASIO). However, the two warrant types will be subject to significant differences in their respective issuing authorities, issuing criteria, and reporting requirements. In particular:

[186] *Submission to the PJCIS Review of the TOLA Act*, (October 2019), 4 at [3.1].
[187] Ibid. See also: Richardson Review, *Unclassified Report: Volume 3*, (December 2019), recommendation 173 (largely endorsing the submissions of the IGIS in relation to access to independent expertise for oversight purposes, and supporting the establishment of an independent panel of experts to assist the IGIS as needed).

- **issuing authorities**—network activity warrants will be issued by eligible judges or AAT members, whereas ASIO's warrants are issued internally, by a Minister (the Attorney-General);[188]
- **issuing criteria**—issuing authorities for network activity warrants are required to be satisfied there are reasonable grounds for the AFP or ACIC's suspicion that the issuance of the warrant would substantially assist in the collection of the specified intelligence; and must also have regard to specified matters that are directed to proportionality. These requirements are to assess, in all cases, the nature and gravity of the relevant offence; the value of the intelligence sought; whether the things sought to be authorised are proportionate to the likely intelligence value; the existence of less intrusive collection methods; the extent to which the data of non-suspects may be accessed; and any previous warrants sought or issued.[189]

  In contrast, for ASIO's warrants, the Attorney-General need only be satisfied that there are reasonable grounds for believing that access by ASIO to data held in a computer will substantially assist in the collection of intelligence in relation to a security matter.[190]

  While the Minister's Guidelines to ASIO, issued under section 8A of the ASIO Act, require ASIO to apply a proportionality assessment to its decisions to exercise its intrusive powers,[191] this is far more limited than a statutory issuing criterion directed to proportionality, because, as the Law Council has observed previously:[192]

  - the guidelines are only administratively binding on ASIO, in that an independent assessment of proportionality is not a legal pre-condition to the authorisation of a power, or a legal limit on the scope of a power; and

  - the guidelines are not a legislative instrument, and can be varied unilaterally by the executive government at any time; and

  - the current direction in the guidelines with respect to proportionality appears to focus on the right to privacy. While important, this is not the only relevant consideration to a proportionality assessment. For example, rights to equality and non-discrimination can also be engaged through target selection; and

- **public reporting requirements**—network activity warrants will be subject to a public annual reporting requirement, under which the Parliament must be provided with the number of network activity warrants sought by, and issued to, the AFP and ACIC. It must also be given information about the kinds of offences in relation to which intelligence was obtained under network activity warrants.[193] In contrast, all of ASIO's reports on special powers warrants are classified and are not subject to public disclosure.[194]

494. As also noted above, these differences in the two warrant regimes are anomalous given the realistic possibility for significant overlap between the subject-matter

---

[188] Bill, Schedule 2, item 9 (inserting proposed subsection 27KK(3) of the SDA). Cf ASIO Act, subsection 25A(1).

[189] Bill, Schedule 2, item 9 (inserting proposed subsections 27KM(1) and (2) of the SDA).

[190] ASIO Act, subsection 25A(2).

[191] The Hon Peter Dutton MP, Minister for Home Affairs, *Minister's guidelines in relation to the performance by ASIO of its functions and the exercise of its powers,* (August 2020), 11-12 at [3.4].

[192] Law Council of Australia, *Pro-active submission to the Minister for Home Affairs, Attorney-General and PJCIS Chair on the Minister's Guidelines to ASIO*, (August 2020).

[193] SDA, subsection 50(1) and Bill, Schedule 2, item 24 (inserting proposed paragraph 50(1)(eb) of the SDA).

[194] ASIO Act, section 94.

covered by network activity warrants and ASIO computer access warrants, where the suspected activities of the target constitute or facilitate an offence and a threat to security. This possibility is significant in relation to offences against the security of the Commonwealth (including terrorism and foreign incursions), and offences in the nature of foreign interference or espionage. The extrinsic materials to the Bill do not appear to address this broader matter of legislative inconsistency in relation to the requirements for issuing and reporting on similar warrant types.

495. The Law Council considers that the potential for significant overlap between the respective intelligence-collection powers of the AFP and ACIC, and ASIO, cast doubt on the continued appropriateness of maintaining extensive legislative differences in the respective issuing authorities, issuing criteria and public reporting requirements for both warrant types.

496. If the AFP and ACIC are to be given a discrete power to exercise intrusive powers for intelligence collection purposes in circumstances where there is likely to be significant overlap with ASIO's powers, then consideration should be given to improving the alignment of ASIO's equivalent intelligence collection powers with the stronger legislative safeguards contained in the network activity warrant regime.

Recommendation 40—re-consideration of the issuing process and thresholds for ASIO computer access warrants, to better align with network activity warrants

- **Further consideration should be given to whether there is a compelling, principled basis for retaining distinctions between the issuing and public reporting requirements for ASIO's computer access warrants, and network activity warrants for the AFP and ACIC, in view of the potential for significant overlap in the subject-matter covered by both warrant types. (That is, where the 'relevant offence' for a network activity warrant also falls within the definition of 'security' in the ASIO Act, as is the case with, for example: terrorism, foreign incisions, foreign interference and espionage offences.)**

Account takeover warrants (Schedule 3)

497. Schedule 3 to the Bill proposes to amend the Crimes Act to insert new Part IAAC. This will establish the third new type of warrant-based power of AFP and ACIC, known as 'account takeover warrants'. These warrants would authorise the AFP to effectively 'lock out' the owner of one or more online accounts for a maximum of 180 days, for the purpose of investigating one or more 'relevant offences'.

498. The Bill proposes to define a 'relevant offence' for the purpose of the account takeover warrant regime by incorporating the existing definition of a 'serious Commonwealth offence' in Part IAB of the Crimes Act (for the purpose of the controlled operations regime).[195] This covers an offence against a law of the Commonwealth that is punishable by a maximum penalty of three or more years' imprisonment.[196] This is equivalent to the definition of a 'relevant offence' under section 6 of the SDA (discussed above).

499. Account takeover warrants would be issued by a magistrate who is appointed in a personal capacity, on the application of a 'law enforcement officer' of the AFP or

[195] Bill, Schedule 3, item 4 (inserting proposed section 3ZZUK of the Crimes Act).

[196] Ibid, Schedule 3, item 4 (inserting proposed section 3ZZUK of the Crimes Act, which incorporates by reference the definition of a 'serious offence' in Part IAB of the Crimes Act in relation to controlled operations. See existing subsections 15GE(1) and (3) of the Crimes Act).

ACIC.[197] A 'law enforcement officer' is defined broadly to include, among other persons, an employee or special member of the AFP, a secondee to the AFP, and a member of staff of the ACIC (which includes secondees), without any requirement to be individually authorised by the agency head or another senior officer.[198]

500. A magistrate may issue an account takeover warrant if satisfied of the following matters:

- there are reasonable grounds for the suspicion of the applicant that:
  - one or more 'relevant offences' have been, are being, are about to be, or are likely to be, committed;
  - an investigation into those offences is being, will be, or is likely to be conducted; and
  - taking control of one or more 'online accounts' (the 'target accounts') is necessary for the purpose of enabling evidence to be obtained of the commission of those offences; and
- it is appropriate to issue the warrant, having regard to:
  - the nature and gravity of the relevant offences;
  - the existence of alternative means of obtaining the relevant evidence;
  - the extent to which the privacy of any person is likely to be affected;
  - the likely evidentiary value of any evidence sought to be obtained;
  - any previous account takeover warrants sought or issued in connection with the same online account, or the same relevant offences.[199]

501. There is no requirement for applications to be accompanied by a sworn affidavit setting out the relevant facts. Rather, the application must provide 'sufficient information to enable the magistrate to decide whether or not to issue the warrant'.[200]

502. An 'online account' is defined as an 'account that an electronic service has for an end user'. The component terms 'account' and 'electronic service' are defined by reference to the meaning of those terms in the *Enhancing Online Safety Act 2015* (Cth) (**EOSA**), namely:

- **account**—this term is defined to include both free and pre-paid accounts, and 'anything that may reasonably be regarded as the equivalent of an account'. (The term 'account' itself is not defined exhaustively in the EOSA).'[201]
- **electronic service**—this term is defined to mean:
  - a service (which includes a website) that allows end-users to access material using a carriage service; or

[197] Ibid, Schedule 3, item 4 (inserting proposed subsection 3ZZUN(1) of the Crimes Act).
[198] Ibid, Schedule 3, item 4 (inserting proposed section 3ZZUK of the Crimes Act).
[199] Bill, Schedule 3, item 4 (inserting proposed section 3ZZUP of the Crimes Act).
[200] Ibid, Schedule 3, item 4 (inserting proposed subsection 3ZZUN(3) of the Crimes Act).
[201] EOSA, section 4.

- a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service; but

- does not include a 'broadcasting service' or a 'datacasting service' within the meaning of the *Broadcasting Services Act 1992* (Cth).[202]

503. An account takeover warrant may be in force for up to 90 days, with the ability to obtain an extension for a further 90 days (or 180 days in total).[203] Under proposed section 3ZZUR or the Crimes Act, an account takeover warrant may authorise any of the following activities, as the magistrate considers appropriate in the circumstances:

- taking control of the account, if doing so is necessary to obtain evidence (under a separate source of legal authority) about the commission of the relevant offence or offences in respect of which the warrant is issued. 'Taking control' is defined in proposed section 3ZZUL to mean the AFP or ACIC having exclusive access to the account—including by using existing account credentials to alter one or more of those credentials or to change the kinds of account credentials required, or removing multi-factor authentication;
- using a computer, a telecommunications facility, or other electronic equipment or a data storage device for the purpose of taking control of the account;
- if necessary to take control of the account, accessing relevant account-based data, or adding, copying, deleting or altering account credentials or other data in a computer;
- if, having regard to other methods that are likely to be as effective, it is reasonable in all the circumstances—using a communication in transit for the purpose of taking control of the account (and adding, copying, deleting or altering data in the communication in transit);
- concealing the fact that any act or thing was done under the warrant, including 28 days (or more) after the cessation of the warrant; and
- causing loss of, or damage to, data provided that this is justified and proportionate having regard to the relevant offence or offences specified in the warrant.

504. Importantly, account takeover warrants do not authorise the collection of evidence of the relevant offence. This would require authorisation under a separate warrant (such as a computer access warrant). This tends to suggest that account takeover warrants would likely be sought and executed as part of a suite of warrants authorising multiple powers in relation to suspected cyber-enabled offending. Further, any covert use of the account by the AFP or ACIC would require separate authorisation (for example, as part of a controlled operation, or potentially under an authority to use an assumed identity).

505. The Bill also proposes to confer a limited right to obtain statutory compensation from the Commonwealth, if a person suffers loss of or serious damage to property (including data), or personal injury, in the course of or as a direct result of the execution of an account takeover warrant.[204]

[202] Ibid, section 4.

[203] Bill, Schedule 3, item 4 (inserting proposed subsection 3ZZUQ(3) and proposed paragraph 3ZZUS(1)(a) of the Crimes Act).

[204] Ibid, Schedule 3, item 4 (inserting proposed section 3ZZWA of the Crimes Act).

506. When an account takeover warrant ceases to be in force, the AFP or ACIC are obliged to take all reasonable steps to restore the account-holder's access to the account, if satisfied that it is lawful for the person to operate that account.[205]

507. The Ombudsman would be responsible for conducting oversight of the actions of the AFP and ACIC in obtaining and executing account takeover warrants, including a specific power of inspection of these agencies' compliance with the requirements of new Part IAAC of the Crimes Act.[206]

508. Schedule 3 to the Bill further proposes to confer a power on the AFP and ACIC to obtain mandatory assistance orders, which can be used to compel a wide range of people to render assistance in executing the warrant. This includes a suspect, an account holder (or an employee or contractor), and account user, or a system administrator—provided that any such person has relevant knowledge of the account or electronic service, or protective measures applied to account-based data.

509. These persons can be compelled, under penalty of an offence punishable by a maximum of 10 years imprisonment, to provide 'any assistance that is reasonable and necessary to allow the law enforcement officer to take control of an online account' pursuant to an account takeover warrant.[207] This would appear to cover the communications and technology companies that provide account-based electronic communications services, such as social media and messaging platforms.

Similar issues to data disruption and network activity warrants

510. Several of the issues raised above in relation to data disruption warrants and network activity warrants apply similarly to account takeover warrants. Consequently, the Law Council makes the below recommendation in relation to these aspects of the proposed warrant-based account takeover regime.

Recommendation 41—amendments to account takeover warrant regime to address common or similar issues across all three new warrant types

- **The account takeover warrant provisions in proposed Part IAAC of the Crimes Act (Schedule 3 to the Bill) should be amended in line with previous recommendations in this submission concerning data disruption or network activity warrants (or both) with respect to the following matters:**
  - **the definition of a 'relevant offence' for the purpose of account takeover warrants should be aligned with the Law Council's recommendation 3 above;**
  - **the 'law enforcement officers' of the AFP and ACIC who may apply for account takeover warrants should be limited to staff members of a minimum classification, who have been specifically authorised by the AFP Commissioner or ACIC CEO (as applicable). The statute should not automatically authorise all staff AFP and ACIC members to be applicants;**
  - **the issuing authority for account takeover warrants should be a superior court judge, appointed *persona designata*; and**

[205] Ibid, Schedule 3, item 4 (inserting proposed section 3ZZUV of the Crimes Act).
[206] Ibid, Schedule 3, item 4 (inserting Division 7 of proposed Part IAAC of the Crimes Act).
[207] Ibid, Schedule 3, item 4 (inserting proposed section 3ZZVG of the Crimes Act).

- **any ability to engage in post-warrant concealment activities more than 28 days after an account takeover warrant has ceased to be in force should require independent authorisation.**

- **The mandatory assistance order regime for account takeover warrants in proposed section 3ZZVG of the Crimes Act (Schedule 3 to the Bill) should be amended in line with equivalent recommendations of the Law Council for other types of assistance orders. In particular:**
  - **The issuing criteria for mandatory assistance orders should require consideration of whether the person is, or has been, the subject of any previous mandatory assistance orders (under multiple regimes);**
  - **there should be an explicit requirement for all mandatory assistance orders to specify material particulars, including the date or time period over which the assistance must be rendered and the nature of the relevant assistance; and**
  - **mandatory assistance orders should be subject to the same reporting and record-keeping obligations as the underlying account takeover warrant.**

Issues specific to account takeover warrants

511. The balance of the Law Council's comments on Schedule 3 to the Bill focus on the following matters, which are specific to the account takeover warrant regime:
    - the necessity of an account takeover power, in light of:
      - existing warrant-based computer access and data surveillance powers under the SDA; and
      - existing compulsory assistance powers in relation to computer access warrants and the industry assistance regime in Part 15 of the Telecommunications Act;
    - the breadth of the proposed definition of an 'electronic service' as a component of the definition of an 'online account' that may be the subject of a takeover warrant;
    - the absence of a requirement for all account takeover warrant applications to be supported by a sworn affidavit by the AFP or ACIC applicant, with a limited exception for emergency circumstances (consistent with the proposed requirements for data disruption and network activity warrants, and the existing requirements for computer access and surveillance device warrants);
    - further matters relevant to the proportionality of the proposed account takeover powers, including:
      - the total duration of an account takeover warrant, as a maximum of 180 days (including an extension of up to 90 days), in combination with:
        - the absence of a clear prohibition on account takeover warrants authorising repetitive takeovers of an individual online account for the total period of effect of that warrant; and
        - the absence of any limits on the number of consecutive account takeover warrants that may be issued in relation to a single online account;

- the absence of an issuing criterion directed to the proportionality of the broader impacts of the account takeover powers on both the target and other persons, in addition to the limited proposed obligation to assess only the anticipated privacy impacts;
- the conferral of a power on the AFP and ACIC to cause loss of, or material damage to, data in the course of executing an account takeover warrant, if this is assessed by the AFP or ACIC officers executing the warrant as being 'justified and proportionate' to the object of the warrant;
- the conferral of a narrow statutory compensation right against the Commonwealth. This is limited to persons who suffer loss, damage or injury as a direct result of the execution of an account takeover warrant by the ACIC or AFP (thereby excluding so-called 'relational loss' which is sustained by persons who were not the account-holder or user, but were reliant on the account-holder operating the relevant account to provide information, or goods such as digital currency, or other services, and suffered loss as a result of the account takeover); and
- the absence of a requirement to notify people who are 'locked out' of an online account (including provisions for notification on a delayed basis, if 'real-time' disclosure is assessed as likely to cause serious prejudice to the investigation, or to the life, health or safety of another person);

- the broad, discretionary exemptions from the obligation on the AFP and ACIC to restore a person's access to an online account, after the account takeover warrant ceases to be in force. In particular, the restoration obligation does not apply if the AFP or ACIC unilaterally forms a view that it is not lawful (for any reason) for the holder of a target account to operate that account; and
- limitations in oversight arrangements, including:
  - the absence of a requirement for the Ombudsman (and Minister) to be notified if the AFP or ACIC do an act in purported compliance with an account takeover warrant, which has caused, or is assessed as being reasonably likely to cause, material loss, damage, harm, injury or interference to a third-party; and
  - the limitation of the Ombudsman's inspection function to an examination of the compliance by the AFP or ACIC with the statutory requirements of the new warrant-based regime, to the exclusion of a broader function to consider matters of propriety (equivalent to that of the IGIS).

Necessity of coercive account takeover powers

512. The Explanatory Memorandum provides limited justification for the proposal to confer coercive account takeover powers. It notes that law enforcement agencies can presently only takeover a person's account with that person's consent. It indicates that the proposed warrant-based regime is intended to address this 'gap' in existing powers.[208] However, it does not explain why the proposed extension of powers is necessary, in light of the following investigative powers:

    - existing electronic surveillance powers that would authorise access to (under computer access warrants, and surveillance device warrants authorising the use of data surveillance devices) to monitor a person's online activities using an account, for the purpose of obtaining evidence of a suspected 'relevant offence';

[208] Explanatory Memorandum, 5 at [22]-[23].

- the existing power to obtain mandatory assistance orders in respect of computer access warrants, which can require third parties to render assistance in gaining access to data and making it intelligence to law enforcement agencies;
- the existing industry assistance powers in Part 15 of the Telecommunications Act, under which the online account providers could be requested ('technical assistance requests') or compelled ('technical assistance notices') to provide technical assistance or capability, and will receive immunity from criminal or civil liability in respect of that assistance; and
- the potential ability to obtain authorisation as part of a controlled operation.

513. In particular, the Explanatory Memorandum does not identify the precise objective underlying the proposed power to lock a person out of an online account (potentially permanently, if the AFP or ACIC self-assess that the access restoration obligation does not apply), in addition to covertly monitoring the person's activities using that account. For example, is the underlying objective of gaining exclusive control of the account to prevent the apprehended destruction of evidence by the target? Or is the underlying objective, in fact, to frustrate the commission of a relevant offence using that account?

514. The Law Council suggests that the proposal to confer a new and extraordinary power, which has the potential to cause significant loss and damage to third parties who are not under any suspicion of wrongdoing, should not proceed unless and until a detailed and specific justification is provided, and is scrutinised by the Parliament and wider community.

515. Moreover, if the underlying policy objective is evidence preservation, this should be written explicitly into the issuing criteria for data disruption warrants, so that the issuing authority is required to assess the likely effectiveness of a proposed warrant in achieving this specific objective.

Recommendation 42—justification for coercive account takeover powers

- **The proposed account takeover warrant regime in Schedule 3 to the Bill should not proceed unless and until a detailed justification of the perceived necessity is provided publicly, and the Parliament and public have an adequate opportunity to scrutinise it.**
- **This justification should provide specific reasons for the perceived necessity of a power to lock a person out of their account, in addition to existing electronic surveillance powers to monitor the person's activities using that account.**
- **If the objective is to preserve evidence of a suspected 'relevant offence', by preventing its destruction by the account holder or others with access to the account, then this should be explicitly incorporated in the issuing criteria for account takeover warrants.**

Definition of an 'online account'

516. An 'online account' and its component term 'electronic service' are extremely broad, effectively requiring the provision of an electronic service (through means of a carriage service, such as the internet) to a registered end user.[209] This could potentially cover most online services used by large numbers of people in

[209] Bill, Schedule 3m item 4 (inserting definitions in proposed section 3ZZUK of the Crimes Act.

conducting their ordinary personal and business affairs, such as the following account-based services that are commonly accessed via desktop websites or apps:

- communications services (such as social media, email, and voice and data messaging accounts);
- online information and communication systems used by businesses for the purpose of employees working remotely;
- news and media (such as web or app-based access to news platforms);
- cloud-based data storage and processing accounts (including accounts linked to systems utilised by businesses, to enable staff to work remotely);
- banking and financial services (such as web or app-based bank, insurance or superannuation accounts);
- utilities (such as web or app-based electricity or water accounts);
- government services (such as those linked to MyGov, including web or app-based customer accounts for Medicare, Services Australia, and the Australian Taxation Office);
- enrolment-related portals for educational institutions (such as web or app-based school or university accounts).

517. Accordingly, it would be possible for a single account takeover warrant to authorise the AFP or ACIC to 'lock out' a person from multiple accounts, including those accounts which provide essential services to their customers, if they are suspected of being connected, in some way, with the commission of a 'relevant offence'. In this context, it is also important to note practical trends in the uptake and use of electronic services falling within the proposed definition of an 'online account'. In particular, the COVID-19 pandemic has necessitated the conduct of an increasing number of personal and business transactions via online means (particularly remote work). This circumstance is material to the breadth of coverage of the proposed regime and, in turn, its proportionality. In considering the proportionality of the proposed account takeover power, it is also important to consider this issue in combination the 'relevant offences' in respect of which warrants can be issued.

518. The Law Council notes that the Explanatory Memorandum does not provide insight into the key types of 'online accounts' that gave rise to the perceived need for an account takeover power. The Law Council recommends that consideration is given to amendments which will:

- reduce the scope of the proposed definition of an 'online account' to accounts connected with electronic communications services. This could potentially be given effect in a similar manner to the communications services covered by the definition of 'designated communications provider' for the purpose of the proposed international production orders in the Telecommunications Legislation Amendment (International Production Orders) Bill 2020;[210] or
- alter the issuing criteria for account takeover warrants, to apply specific exclusions or limitations for online accounts that are, or are likely to be, essential services (such as personal or business banking or other financial services, and governmental services that are delivered via an online account).

Recommendation 43—definition of an 'online account'

[210] Telecommunications Legislation Amendment (International Production Orders) Bill 2020, Schedule 1, (inserting proposed Schedule 1 to the TIA Act, clause 2—definition of 'designated communications provider, relevantly covering telecommunications carriers and carriage service providers; and 'message/call application service providers' and 'general electronic content service providers').

- **The definition of an 'online account' and its component term 'electronic service' in proposed section 3ZZUK of the Crimes Act (item 4 of Schedule 3) should be amended to cover a more limited sub-set of online accounts, such as social media, email, and data or voice messaging accounts.**
- **However, if there is no intention to limit the definition of an 'online account' in this way, the issuing criteria for account takeover warrants in proposed section 3ZZUP of the Crimes Act (item 4 of Schedule 3) should apply specific exclusions or limitations in relation to online accounts that are used to provide essential services to a person, such as banking and governmental services.**

Absence of requirement for affidavits

519. Proposed section 3ZZUN of the Crimes Act does not include a requirement for account takeover warrant applications to be accompanied by an affidavit, setting out the facts and grounds of the application. The Explanatory Memorandum does not explain why such a requirement has not been included.

520. The absence of such a requirement seems anomalous, given that account takeover warrants have been designed to operate in combination with other warrants to authorise data access (such as computer access warrants) which require affidavits other than in circumstances of emergency.[211] The requirement for an affidavit is an important form of assurance in relation to the rigour, precision and internal approval requirements for warrant applications. This is particularly important given the proposal to enable any 'law enforcement officer' of the AFP or ACIC to make an application for these warrants.

521. Given the intrusive, broad and novel nature of account takeover powers, the Law Council recommends that proposed section 3ZZUN should be amended to require all warrant applications to be accompanied by an affidavit.

Recommendation 44—requirement for affidavits

- **Proposed section 3ZZUN of the Crimes Act (item 4 of Schedule 3) should be amended to require all applications for account takeover warrants to be accompanied by a sworn affidavit, setting out the facts and grounds on which the warrant application is based.**

Duration of account takeover warrants

522. Account takeover warrants have a maximum duration of 90 days, which can be extended for up to a further 90 days (a total of 180 days, or six months).[212] This is a lengthy period during which a person could be locked out of an online account and unable to operate it, especially view of the wide range of accounts covered by the proposed regime (including account-based essential services delivered online).

523. The Explanatory Memorandum does not appear to provide reasons for the selection of the proposed maximum period of effect for these warrants. The Law Council cautions against selecting a maximum period of effect on the basis of alignment with other warrant types. Rather, the maximum period of effect for a warrant authorising

[211] See, for example, SDA, paragraph 27A(8)(b).

[212] Bill, Schedule 3, item 4 (inserting proposed subsection 3ZZUQ(3) and proposed paragraph 3ZZUS(2)(a) of the Crimes Act).

an intrusive or coercive power should be demonstrably necessary for, and proportionate to, the exercise of the particular powers conferred under that warrant.

524. The Law Council acknowledges that proposed section 3ZZUU obliges the AFP Commissioner or ACIC CEO to revoke a warrant, if satisfied that taking control of an account is no longer required for the purpose of enabling evidence to be obtained of the commission of the relevant offence or offences specified in the warrant. However, if a revocation is not made for any reason, the warrant will remain in force until it expires (noting the maximum duration of up to 180 days, if extended). Further, circumstances could potentially arise in which the AFP or ACIC may consider it necessary to repeatedly exercise account takeover powers at various points over a long period of time, to intermittently obtain evidence of a suspect's offending. (For example, in relation to offences which cover a continuing course of conduct; or in relation to a course of conduct that comprises multiple offences.)

525. Given the intrusive nature of account takeover powers, and the potential to cause significant loss or disruption to individual account holders and others, the Law Council suggests that account takeover powers should be treated in a manner that is more closely aligned with search warrants under existing provisions of the Crimes Act. In particular, search warrants must be executed within seven days of issuance, and are spent when the search of the specified premises is complete.[213] A further search of the same premises, in relation to the same suspected offence, will generally need authorisation under a new warrant.[214]

Recommendation 45—duration of warrants and authorisation of repetitive acts

- **Proposed subsection 3ZZUQ(3) of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to provide that an account takeover warrant must be executed within seven days of its issuance, and automatically ceases to be in force once the AFP or ACIC has gained exclusive control of the account (akin to search warrants).**
- **If the AFP or ACIC seek to re-gain exclusive control of that account if that control is lost for any reason, they should be required to obtain specific authorisation from the issuing authority, ideally under a fresh account takeover warrant.**

Assessment of third-party impacts in addition to privacy

526. The Law Council welcomes the specific requirement in proposed paragraph 3ZZUP(2)(c) for the issuing authority to have regard to the likely impacts of an account takeover warrant on the privacy of any person. This would include the privacy of the account holder, and any other person who uses the account, or whose personal information is accessible via the account.

527. However, the Law Council is concerned that this there is no broader obligation to consider third-party impacts in addition to privacy. As noted above, the types of 'online accounts' that could be the subject of a takeover warrant far exceed those which only store personal information. For example:

[213] Crimes Act, subsection 3E(5A).
[214] There is some leeway under section 3JA of the Crimes Act if an officer executing a search warrant has to leave the premises mid-way through a search due to an emergency. However, if the officer is unable to return those premises within a 12-hour period, any re-entry to complete the search requires additional authorisation.

- The issuance of an account takeover warrant in relation to an individual's bank account may mean that a person is unable to transfer funds from that account to pay essential bills and other living expenses for a significant period of time;
- Many individuals' cloud-based data storage accounts contain a variety of documents for a combination of work, educational and personal purposes. The issuance of an account takeover warrant in relation such an account may prevent the account holder, and any others who are authorised to use that account, from completing their employment or educational requirements, or transacting important matters of personal business that require access to documents stored in that account; and
- in the case of account holders who are children or vulnerable persons, or persons who are their caregivers, the takeover of an online account used for the purposes of communicating with family members, or receiving or providing care, may have particular adverse consequences for these individuals.

528. The Law Council acknowledges that it would be open to issuing authorities to exercise their discretion to consider broader third-party impacts when determining individual warrant applications. However, the insertion of a statutory issuing criterion would ensure consistency and certainty about the consideration of third-party impacts in all warrant applications and issuing decisions.

529. The interests of the kind noted above are equally important to privacy rights, and their infringement have even more harmful effects than the loss of privacy. This makes it important that there is clear and consistent statutory guidance for both warrant applicants and issuing authorities.

Recommendation 46—assessment of third-party impacts

- **Proposed subsection 3ZZUP(2) of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to require the issuing authority to consider whether a proposed account takeover warrant is likely to have adverse impacts on third parties.**
- **This should include specific requirements to assess likely:**
  - **impacts on personal privacy**
  - **financial impacts (on individuals and businesses);**
  - **impacts on a person's ability to conduct their business and personal affairs (including employment or education); and**
  - **impacts on a person's ability to have contact with family members, or provide or receive care.**

Power to cause loss of, or damage to, data

530. Proposed paragraph 3ZZUR(8)(a) of the Crimes Act provides that an account takeover warrant must not be executed in a manner that results in loss of, or damage to, data, unless this is 'justified and proportionate, having regard to the relevant offence'. The Explanatory Memorandum states that, 'whether damage is justified and proportionate will need to be a matter considered by the issuing authority on a case-by-case basis'.[215]

531. However, the Explanatory Memorandum does not provide an explanation of the perceived need to authorise the AFP or ACIC to cause such loss or damage.

[215] Explanatory Memorandum, 159 at [925].

Further, it is not clear that proposed paragraph 3ZZUR(8)(a) requires the issuing authority to specifically authorise individual acts that the AFP or ACIC applicant identifies as being likely to cause loss of, or damage to data.

532. Rather, since this provision is a condition on the manner in which an account takeover warrant must be executed, it would appear to place responsibility on the officers executing a warrant to determine whether any loss of, or damage to, data is 'justified and proportionate, in advance of doing a particular act under the warrant that is likely to cause such loss or damage As with the Law Council's above comments on the proposed data disruption powers, the Law Council is concerned that this decision-making would not be subject to specific, external authorisation, and may effectively place the AFP and ACIC in the role of 'judge, jury and executioner'.

Recommendation 47—omission of power to cause loss of, or damage to, data

Preferred option

- **Proposed paragraph 3ZZUR(8)(a) of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to provide that the AFP and ACIC must not execute a warrant in a manner that results in loss of, or damage to, data. There should be no general exception for loss or damage that is considered to be 'justified and proportionate'.**

Alternative (non-preferred) option

- **If the Committee considers there is a compelling justification for authorising the AFP or ACIC to cause loss of, or damage to, data in the course of executing an account takeover warrant, this should be among the powers in proposed subsection 3ZZUR(2) that the issuing authority may individually authorise, if satisfied the applicable issuing threshold is met.**

Limitations in statutory compensation rights

533. The Law Council welcomes the inclusion of the statutory compensation provision in proposed section 3ZZWA of the Crimes Act. This requires the Commonwealth to pay compensation to persons who suffer loss, damage or injury in the course of, or as a direct result, of the execution of an account takeover warrant.

534. However, this statutory compensation right appears to be unduly narrow. It does not extend to people who suffer loss as an indirect result of the execution of an account takeover warrant, even if that loss is reasonably foreseeable to the AFP or ACIC in executing that warrant.

535. This may be the case if, for example, an account takeover warrant is issued in relation to an individual's bank account, and that individual consequently is unable to pay moneys owing to a third-party. In the event that the third-party became aware that the account takeover warrant was the source of the failure to pay, they would be unable to exercise a statutory compensation right under section 3ZZWA. Given that account takeover warrants can remain in force for up to 180 days (inclusive of an extension) there could be a significant possibility for an account takeover to result in financial loss in these circumstances.

Recommendation 48—statutory compensation rights

- **Proposed section 3ZZWA of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended to extend statutory compensation rights to persons who suffer either direct or indirect loss, damage or injury from the execution of an account takeover warrant.**

Absence of notification requirements

536. The Bill does not propose to require the AFP or ACIC to notify an account holder that their account is, or has been, the subject of an account takeover warrant.

537. On one hand, it is understandable that an obligation to provide 'real-time' notification may frustrate a covert investigation. However, the absence of any notification requirement means that an account holder, who may not necessarily be the suspect in relation to a 'relevant offence', could be deprived of access to their account for a prolonged period of time (up to 180 days) without any information about the reasons or causes, and therefore without ability to challenge the legality of the warrant.

538. If the relevant electronic service provider is aware of the warrant (for example, because they have been compelled to provide assistance in executing it, or the AFP or ACIC have made a voluntary disclosure) the secrecy provisions in proposed section 3ZZVH would appear to prevent them from making a disclosure to the account holders or users, as their customers or clients. This could potentially place some electronic service providers in breach of their contractual or other service-level obligations to their users, with respect to the quality and continuity of their account-based electronic services.

539. The Law Council suggests that consideration is given to the insertion of a statutory requirement of general application for the account-holder to be notified that their account has been taken over under a warrant. However, this general rule could be subject to a discretionary power of the issuing authority to make an order providing that the notification may be delayed, or dispensed with permanently, if satisfied on reasonable grounds that this is necessary to avoid frustrating an investigation, or jeopardising the life or safety of any person.

Recommendation 49—notification requirement

- **Schedule 3 to the Bill should be amended to:**
  - **require the AFP or ACIC to notify an account holder that their account is the subject of an account takeover warrant; and**
  - **authorise the issuing authority to make an order, on the application of the AFP or ACIC, to either delay or dispense with the notification requirement, if satisfied on reasonable grounds that giving notification to the account holder would frustrate an investigation, or jeopardise the life or safety of any person.**

Exceptions to obligations to restore account access

540. The Law Council welcomes the general intent of proposed section 3ZZUV to place obligations on the AFP and ACIC to take all reasonable steps to restore a person's access to an online account when an account takeover warrant ceases to be in force. However, the Law Council is concerned that the proposed conditions for the

enlivenment of that obligation place an overly broad discretion in the AFP or ACIC officers executing the warrant.

541. In particular, proposed paragraph 3ZZUV(b) provides that the obligation applies only if it is lawful for the account holder to operate the account. The Law Council is concerned that this provision places the AFP or ACIC in the position of unilaterally determining the legality of the existence and use of a person's online account. This may involve making complex judgments about a person's eligibility to hold the particular account, and drawing inferences about the purposes for which the account is used, and judging the legality of those purposes.

542. If the AFP or ACIC determined that the obligation to take all reasonable steps to restore an account-holder's access did not apply, it is possible that it may not be technically possible for the service provider to restore the account holder's access. It may also be impossible for the service provider to inform the account holder of the reasons they cannot access their account, due to the application of the secrecy offences in proposed section 3ZZVH; or the fact that the service provider may not be aware of the warrant.

543. Consequently, the Law Council suggests that the 'reasonable steps' obligation should apply in all cases in which the AFP or ACIC execute an account takeover warrant. If there is a concern that holding the account amounts to an offence, or the account is being operated to commit an offence, then the AFP should exercise separate powers of investigation, arrest and charge in respect of that conduct. The proposed exceptions to the obligation to take reasonable steps to restore account access should not be capable of operating as a substitute for enforcement action.

Recommendation 50—obligation to restore account access

- **Proposed section 3ZZUV of the Crimes Act (item 4 of Schedule 3 to the Bill) should be amended, to**
  - **require the AFP and ACIC to take all reasonable steps to restore an account holder's access, after an account takeover warrant has ceased to be in force;**
  - **remove the requirement in proposed paragraph 3ZZUV(b) for the AFP or ACIC to form a view on whether it is lawful for the account holder to operate the account, and replace this with an ability to apply to an issuing authority for an exemption to the restoration obligation; and**
  - **require the AFP to exercise separate powers of investigation, arrest and charge in relation to any offences that may be committed as a result of the person holding or operating the account (or separately make an application for a confiscation or restraining order under applicable proceeds of crime legislation).**

Limitations in oversight arrangements

544. The Law Council welcomes the proposal to confer a power of inspection on the Ombudsman in relation to the compliance by the AFP and ACIC with the requirements of proposed Part IAAC of the Crimes Act.

545. However, the Law Council recommends that this inspection power is supplemented with several measures to ensure its effectiveness, and maximise the degree of assurance provided to the Parliament and the public. In particular, the following

requirements would more effectively enable the Ombudsman to focus oversight on high-risk activities, and conduct comprehensive oversight:

- the reporting and record-keeping requirements for account takeover warrants in proposed Division 6 of new Part IAAC should be extended to cover mandatory assistance orders issued under proposed section 3ZZVG;
- the AFP and ACIC should be required to notify the Ombudsman if they cause loss or damage to a third-party, either in contravention of the limits of authority of a warrant, or pursuant to proposed paragraph 3ZZUR(8)(a); and
- given the broad scope of application of account takeover warrants and the novel nature of this intrusive power, consideration should be given to conferring a broader inspection function on the Ombudsman to consider the propriety, as well as legal compliance, of the activities of the AFP and ACIC under those warrants. (This would be equivalent to the functions of the IGIS in relation to intelligence agencies.)

Recommendation 51—Ombudsman oversight of account takeover warrants

- **The oversight functions of the Ombudsman in relation to account takeover warrants should be enhanced to incorporate the matters listed at paragraph [545] of this submission.**

Overarching matters concerning data disruption, network activity and account takeover powers (Schedules 1-3)

Absence of protections for legally privileged and confidential journalistic information

546. The Law Council has commented previously on the absence of protections in investigative warrant provisions for information that is subject to client legal privilege, and confidential journalistic information.[216]

547. In its inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (**'press freedoms inquiry'**), the Committee also recommended stronger protections for journalistic information in the context of existing surveillance warrants.[217]

548. All three new warrant types in the Bill raise the same issues as those previously identified by the Law Council and the Committee because they also possess the following attributes:

- the 'relevant offences' covered by the new warrant types include secrecy offences which are capable of application to journalists, and lawyers and their clients;
- the new warrant types would also enable data to be accessed from a computer of a person who is not the suspect or target, which could include

[216] In its submissions on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth), the Law Council recommended that the powers conferred under that regime should be subject to specific protections for such information. See: Law Council of Australia, *Supplementary submission to the PJCIS inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020*, (May 2020), 2-5.

[217] PJCIS, *Report on the press freedoms inquiry,* (August 2020), especially recommendation 2 (role of public interest advocates, and issuing by superior court judges in warrants sought against journalists).

journalists and potentially lawyers who are communicating with sources or clients. This risk is exacerbated by:

- the extremely broad range of 'relevant offences' in respect of which the new warrant types may be issued, including offending at the lower end of the range of objective seriousness; and

- the definition of a 'criminal network' for the purpose of network activity warrants (which, as noted above, appears capable of including people who passively interact with an electronic service that is also used by persons who are committing, or facilitating others to commit, a 'relevant offence'); and

- the new warrant types would authorise access to data that is held in, or is accessible from, a computer (for example, a cloud storage drive or a physical hard drive in a computer some or all of which may be privileged, or include confidential journalistic source information. This includes an explicit authority to access data to determine whether it is relevant to the warrant;

549. Consequently, the Law Council recommends that they are also subject to equivalent safeguards. In particular, the following protections should be incorporated:

Information subject, or likely to be subject, to client legal privilege

- In relation to information that is subject to client legal privilege, or is reasonably likely to be subject to a claim for such privilege:
  - the warrant applicant must specifically declare either of the following matters (as applicable):
    - the applicant believes on reasonable grounds that the data to which access is sought, or any other data that may be visible in the course of executing the warrant, is not and does not include, information that is subject to client legal privilege, or information that may be subject to a claim for such privilege. This claim could then then be tested by the issuing authority;[218] or
    - if the applicant believes on reasonable grounds that the data sought is, or includes, information that is subject to client legal privilege, or may be subject to a claim for such privilege (for example, because there is an intention to access communications to and from a lawyer, or a party who is known to be involved in legal proceedings) then they must substantiate the following matters, in addition to the existing issuing criteria for the relevant warrant type, as proposed in the Bill as drafted:
      i. access to privileged information is necessary to execute the warrant (that is, it would not be possible to execute the warrant without access to that information);
      ii. the public interest in accessing the information and investigating or frustrating an offence outweighs the

[218] This is consistent with the Law Council's recommendations in relation to International Production Orders, which is drawn from the equivalent legislation of the United Kingdom. See: Law Council of Australia, *Supplementary submission to the PJCIS inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020*, (May 2020), 2-3.

interest in protecting the confidentiality of lawyer-client communications; and

iii. adequate procedures have been implemented to segregate and protect information subject to a claim or likely claim of client legal privilege, and for such a claim to be made;[219]

- the issuing authority must not issue a warrant unless satisfied of the matters in the above point (as applicable); and

- the default position should be that the person who owns the data being accessed should have an opportunity to be informed of access, unless the issuing authority makes an order preventing disclosure. Such an order may only be made if the issuing authority is satisfied, on reasonable grounds, that disclosure would be reasonably likely to frustrate the objective of the warrant. In this event, the order should be subject to a fixed period of effect, such that the notification requirement will effectively be deferred until after that period.

Journalistic information, including confidential source identities

- In relation to journalistic information (consistent with the Committee's recommendations in its press freedoms inquiry):
  - there should be a role for a public interest advocate in all warrant applications;
  - if the Law Council's recommendations for all warrants to be issued by a superior court judge is not adopted, then at least warrants sought in relation to journalists in relation to actions undertaken in that capacity should be determined by a superior court judge; and
  - the reporting and notification requirements recommended by the Committee should be extended to the new warrant types.[220]

Recommendation 52—specific protections: privileged & journalistic information

- **The issuing criteria and process for all three new warrant types should be subject to the protections listed in paragraph [549] of this submission, in relation to information subject to client legal privilege, and confidential journalistic information (including source identities).**

Potential exposure to multiple mandatory assistance orders

550. In addition to the matters noted above, which are common to all of the existing and proposed forms of mandatory assistance orders, the Law Council is concerned that

[219] This is additional to the Law Council's recommendations in relation to international production orders. It recognises that there may be circumstances in which there is a need to access privileged information for intelligence-related purposes. However, the Law Council recommends that there are explicit criteria directed to the necessity and proportionality of such access.

[220] PJCIS, *Report on the press freedoms inquiry,* (August 2020), recommendations 1-5. (These include requirements to inform journalists when they are no longer persons of interest, reporting and record-keeping requirements in relation to the appointment of persons as public interest advocates to act as contradictors in applications for warrants against journalists, and specific annual reporting requirements in relation to warrants sought or issued against journalists).

the Bill does not contain statutory safeguards against the risk of oppression arising from the potential issuance of multiple, separate assistance orders against a person.

551. For example, there is no requirement for the AFP or ACIC to inform the issuing authority as to whether the subject of an intended mandatory assistance order for a network activity warrant has also been, or could be, compellable under other types of mandatory assistance order. Similarly, there is no such requirement for other types of proposed or existing mandatory assistance order. Consequently, there is also no statutory requirement for the issuing authority to routinely assess this matter in all applications for mandatory assistance orders.

552. The risk of oppression is particularly significant given that:

- the Explanatory Memorandum to the Bill specifically identifies an intention for the three new warrant types to operate cumulatively in a single investigation into serious cyber-enabled crime, including in combination with all existing warrant-based powers (such as computer access and telecommunications interception warrants). In particular, the Explanatory Memorandum contemplates that information obtained under a network activity warrant could be used as the basis for an application for an investigative warrant (such as a computer access warrant) or a data disruption warrant;[221]
- applications for mandatory assistance orders are heard on an *ex parte* basis, with no opportunity for the involvement of an independent contradictor, who could raise this issue, as part of their broader functions to test the case advanced for the issuance of the order; and
- there is a significant maximum penalty of 10 years' imprisonment for the contravention of each mandatory assistance order issued against a person. This means that a person who is subject to multiple, overlapping or substantially similar mandatory assistance orders will be exposed to liability to multiple offences, each of which carry a 10-year maximum penalty.

Recommendation 53—safeguards against exposure to multiple assistance orders

- **The Bill should be amended to insert further statutory pre-conditions to the issuance of all types of mandatory assistance orders under the SDA (existing and proposed), TIA Act, Crimes Act and Part 15 of the Telecommunications Act to require the issuing authority to consider:**
  - **the number of previous orders sought or issued in relation to the subject of a proposed order (by any agency); and**
  - **the likely cumulative impact on the person of being subject to multiple orders, and any third parties whose interests may be affected. (This may include, for example, the employer of a person, whose employee may be unavailable from their usual duties in order to comply with an order).**

[221] See, for example, Explanatory Memorandum, 92 at [465]-[466].

Statutory judicial review of decisions to issue warrants

Apparent error in the Explanatory Memorandum

553. The Explanatory Memorandum states that decisions under the new warrant-based powers, including issuing decisions, will be excluded from statutory judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (**ADJR Act**).[222]

554. This statement appears to be incorrect. The Bill does not propose to make any consequential amendments to Schedule 1 of the AJDR Act to prescribe decisions under the new warrant provisions of the SDA and Crimes Act as decisions to which the ADJR Act does not apply. No such exclusion presently exists. Rather, section 9A of the ADJR Act provides that, when a prosecution or an appeal arising from a prosecution is before a court, there is no jurisdiction to hear and determine an application brought under the ADJR Act for the review of a 'related criminal justice process' decision.[223] This term includes, among other matters, 'decisions in connection with the issue of a warrant'.[224]

555. The Law Council therefore welcomes the statement in the submission of the Department of Home Affairs to the Committee's inquiry that the Government intends to issue a correction to the Explanatory Memorandum.[225] The Law Council provides the below information to assist the Committee in ascertaining the effect of section 9A of the ADJR Act, in relation to the three new warrant types proposed in the Bill.

556. Ultimately, the effect of section 9A of the ADJR Act is to defer the exercise of such rights until the prosecution is concluded; or, more commonly, the warrant may be challenged collaterally in the prosecution itself, via a challenge to the admissibility of particular evidence obtained under that warrant. (For example, admissibility may be challenged on the basis of illegality in the collection of that evidence, because the warrant was invalid due to a defect in the issuing decision; or the action which enabled the collection of the particular evidence exceeded the limits of authority under the warrant.)

557. Further, section 9A of the ADJR Act provides that, if an application for ADJR Act review of a decision to issue a warrant is brought before a prosecution is commenced, then the court may grant a permanent stay of that application, on the application of the prosecution. However, the court may only grant a stay if satisfied that the matters that are subject to the ADJR Act review application are more appropriately dealt with in the criminal justice process, and the stay of ADJR Act proceedings will not substantially prejudice the applicant.[226]

558. Section 9A of the ADJR Act therefore enables a case-by-case assessment to be made of the appropriateness of a stay, rather than effecting a wholesale exclusion of statutory judicial review rights in connection with the issuing of law enforcement warrants. The Law Council supports this outcome in relation to the three new warrant types proposed in the Bill. There does not appear to be any compelling reason for treating them differently to the existing types of investigative warrants available to the AFP and ACIC, including under the SDA and Crimes Act.

---

[222] Explanatory Memorandum, 18 at [44].

[223] ADJR Act, subsection 9A(1).

[224] Ibid, subparagraph 9A(4)(a)(iii).

[225] Department of Home Affairs, *Submission to the PJCIS Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, (February 2021), 23 at [111].

[226] ADJR Act, subsections 9A(2) and (3).

559. As noted below, however, the application of section 9A of the ADJR Act to network activity warrants calls into question the continued appropriateness of conferring a wholesale exclusion from ADJR Act review upon all decisions about the issuance and execution of ASIO's warrants, which are also directed to intelligence-collection.

The case for expanding ADJR Act review to cover further intelligence warrants

560. The availability of ADJR Act review rights in relation to the issuance and execution of network activity warrants contrasts with the wholesale exclusion of ASIO's computer access warrants from ADJR Act review.[227] This is so notwithstanding that:

- both warrant types are directed to the collection of intelligence; and
- there is significant scope for overlap between the activities which could be the subject of surveillance under network activity warrants and ASIO computer access warrants, because conduct constituting an offence (particularly a security offence in Chapter 5 of the Criminal Code) may also constitute a security matter under the ASIO Act.

561. The Law Council submits that the conferral of ADJR Act review rights in relation to network activity warrants raises questions about the continued appropriateness of excluding equivalent ASIO warrants from statutory judicial review. The Law Council notes that:

- there are likely to be only limited circumstances in which a person subject to surveillance under an ASIO computer access warrant became aware of that circumstance, given the generally covert nature of ASIO's investigations. (This could arise if, for example, ASIO exceeded the scope of authority under a warrant and caused loss or damage to a person, or obtained a mandatory assistance order under section 34AAD of the ASIO Act to compel a person to provide assistance in the execution of a warrant);
- if a person becomes aware of an ASIO computer access warrant in connection with a prosecution and seeks to commence ADJR Act review proceedings, section 9A of the ADJR Act would provide a mechanism for the court to determine whether any review proceedings should be stayed; and
- in the event that any ADJR Act review proceedings were not the subject of a stay under section 9A, there are numerous mechanisms available for the protection of classified information in ADJR Act proceedings in relation to warrants. This includes:
  - the ability of the Commonwealth Attorney-General to invoke the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth);
  - the ability of the Commonwealth to make a claim for public interest immunity in relation to certain evidence; and
  - the ability of the court to make orders for closed hearings, or for the suppression or non-publication of certain evidence.

562. The former Administrative Review Council (**ARC**) recommended, in its 2012 report on federal judicial review, that:

[227] Ibid, Schedule 1, paragraph (d).

> *… national security considerations may be a reason for excluding ADJR Act review, particularly where sensitive information is involved which increased litigation in the area may potentially expose. However, the Council does not consider that 'national security' should be a blanket reason for an exemption. Each national security exemption should therefore be considered on its own merits, with regard to whether review of the decisions could pose a risk to national security through the disseminated of information through judicial review proceeding.*[228]

563. The ARC further recommended, in relation to the wholesale exemption of decisions made under the ASIO Act:

> *The exemption from the Administrative Decisions (Judicial Review) Act 1977 (Cth) of all decisions under the Australian Security Intelligence Organisation Act 1979 (Cth) in paragraph (d) of Schedule 1 of the ADJR Act should be reviewed.*[229]

564. The significant differences in treatment under the ADJR Act of two similar types of intelligence collection warrants raises questions about whether the information obtained under ASIO warrants is significantly more sensitive than that obtained under network activity warrants, so as to justify a wholesale exclusion from review under the ADJR Act.

Recommendation 54—availability of statutory judicial review rights for all warrant types (including consistent treatment of intelligence warrants)

- **The forthcoming corrections to the Explanatory Memorandum should specifically explain the effect of section 9A of the ADJR Act in relation to the three new warrant types proposed in the Bill.**
- **As the Bill proposes to make a type of intelligence-collection warrant (namely, network activity warrants) subject to statutory judicial review in accordance with section 9A of the ADJR Act, consideration should be given to extending this arrangement to cover some or all other types of intelligence collection warrants, such as ASIO's computer access warrants.**

Sunset clauses and legislative review functions

565. The Bill proposes to confer three extraordinary powers on an indefinite basis, without provision for independent and parliamentary review of the operation of the new legislation (in addition to independent operational oversight of specific activities by the IGIS and Ombudsman).

Sunset clauses

566. The Law Council considers that the novel nature of the proposed powers, the breadth of their proposed scope, and the gravity of their impacts on individuals (potentially including third parties who are not suspects) makes it essential that they are subject to a finite period of effect. This will ensure that such powers do not remain in law for longer than is necessary, and that the Parliament is empowered to determine whether there is a case for renewal (or permanency) on the basis of evidence of their operation during their period of effect.

[228] ARC, *Federal Judicial Review in Australia*, ARC Report 50, (September 2012), 107 at [5.118].

[229] Ibid, 206, recommendation B6.

Review by the INSLM and Committee

567. The Law Council also emphasises the importance of extraordinary powers—such as those proposed in the Bill—being subject to ongoing, independent review to evaluate comprehensively their effectiveness, necessity, proportionality and human rights compatibility.

568. It appears that neither the INSLM nor the Committee will have comprehensive oversight of new warrant-based powers, if enacted. The oversight remit of both entities under the *Independent National Security Legislation Monitor Act 2010* (Cth) (**INSLM Act**) and Part 4 of the ISA will be dependent on the specific offences in respect of which disruption and account takeover warrants are sought and executed. (Namely, terrorism and foreign incursions-related offences, which are only a very small subset of the wide array of offences in respect of which these warrants could be issued.)

569. There is also no clear statutory basis under the INSLM Act or Part 4 of the ISA for the INSLM or the Committee to conduct oversight of the operation of the new regime of network activity warrants for criminal intelligence purposes.

570. Accordingly, the Law Council recommends that the INSLM Act and ISA are amended to make provision for full oversight by the INSLM and Committee of all three new warrant regimes in the Bill. The resourcing of the INSLM should be increased commensurately with these new functions.

Improvements to Commonwealth legislative design policy

571. More generally, the Law Council supports the routine inclusion of statutory provisions requiring the Parliamentary and independent review of the operation of legislation conferring extraordinary powers, after it has been operational for a reasonable period of time (in the range of three-to-five years).[230]

572. The Richardson Review, whose unclassified report was released in December 2020, has recommended that the *Australian Government Legislation Handbook* (**Legislation Handbook**) should be amended, and associated government guidelines should be made, to require all amendments to intelligence legislation to include adequate provision for the independent operational oversight of new and expanded functions and powers, as supplemented by further guidelines to be made by the Attorney-General. This would make such oversight provisions a formal requirement of Commonwealth policy for the design (and scrutiny) of intelligence legislation.[231]

573. The Law Council recommends that, as a complementary measure, the *Legislation Handbook* should be further amended to include requirements for the independent and Parliamentary review of the operation of legislation conferring extraordinary powers. Pending the formal updating of the *Legislation Handbook*, this

[230] See further: Department of the Prime Minister and Cabinet, *Australian Government Legislation Handbook*, (February 2017), 26 at [5.26] which states that, 'in developing new legislation and amending existing legislation, departments will need to consider whether a mechanism for reviewing the legislation could be included'. The Handbook directs departments responsible for developing legislative amendments to consider whether such a review should be one-off or regular/periodic, and to specify the matters that should be considered. It gives examples, including whether the legislation is operating effectively, has resulted in unintended consequences, remains relevant and clear or contains any outdated or redundant provisions.

[231] Richardson Review, *Unclassified Report*, Volume 4, (December 2019), 265-271 at [40.114]-[40.139] and recommendations 170 and 171.

recommendation should be implemented as a matter of good practice in relation to all future security and intelligence-related legislation.

Recommendation 55—sunset clauses and statutory review functions

- **The Bill should be amended to provide that:**
  - **all of the new warrant-based powers are subject to a sunset clause of three years (or a period no more than five years); and**
  - **the Committee is required to conduct a review of these warrant-based powers prior to their sunset date, to inform Parliamentary decision-making about whether they should be renewed**
- **Consideration should be given to expanding the remit and resourcing of the INSLM to cover the operation of the new warrant-based powers in full, including the ability of the Committee to request the INSLM to undertake a review of these provisions, which could inform the subsequent Parliamentary pre-sunsetting review.**
- **Further consideration is needed for independent and Parliamentary oversight arrangements for criminal investigation powers and offences that have national security implications but are not directed exclusively to national security matters. If there is a desire for such functions to be performed by the Committee and the INSLM, then consideration should be given to the necessary legislative amendments and resource increases.**
- **The Australian Government *Legislation Handbook* should be amended to require all proposed national security legislation that seeks to confer new or significantly expanded powers to be subject to the following requirements (particularly in the case of novel or otherwise extraordinary powers, which are coercive or intrusive in nature):**
  - **routine consideration of whether the proposed measures should be subject to a sunset clause, and explicit documentation of the reasons for the ultimate policy decision in the Explanatory Memorandum to the Bill; and**
  - **the routine inclusion of statutory provisions requiring the conduct of independent and Parliamentary reviews after a period of operation, in the range of three to five years.**

Controlled operations conducted online (Schedule 4)

574. Schedule 4 to the Bill proposes amendments to Part IAB of the Crimes Act, with respect to the conduct of controlled operations in the online environment.

575. Essentially, a controlled operation authorises a law enforcement agency to engage in conduct that would otherwise be unlawful, for the purpose of investigating a suspected offence. Part IAB of the Crimes Act also limits the discretion of the court to exclude evidence obtained from a controlled operation, solely because the conduct of the persons involved in the controlled operation would have constituted an offence, but for its authorisation as part of a controlled operation.

576. The proposed amendments in Schedule 4 to the Bill would dispense with certain existing requirements in provisions for the authorisation of controlled operations, where a controlled operation is conducted online. Namely, the Bill proposes to remove the requirement in existing paragraph 15GI(2)(d), and corresponding

provisions in paragraphs (2)(d) of sections 15GQ and 15GV governing variations and extensions, that the authorising officer must be satisfied, on reasonable grounds, that the controlled operation (as authorised, varied or extended):

> *will be conducted in a way that ensures that, to the maximum extent possible, any illicit goods in the controlled operation will be under the control of an Australian law enforcement officer at the end of the controlled operation.*

577. In particular, the proposed amendments would provide that this requirement applies only 'so far as the conduct involved in the controlled operation **is not** conducted online' (emphasis added).[232]

Legal effect of the proposed amendments

578. Despite the suggestion in the Explanatory Memorandum that the proposed amendments are only 'minor',[233] they appear to have a significant legal effect that is material to the following matters:

- the authorisation of law enforcement officers and other covert operatives to engage in activities that would otherwise constitute offences or torts, or both;[234] and
- the exercise of discretion by a court to exclude evidence on the basis that it has been unlawfully or improperly obtained.[235]

Inadequate justification for removing authorisation requirements

579. It is no small measure to authorise agents of the state to engage in otherwise unlawful conduct, and to limit the usual discretion of courts to exclude evidence obtained through such conduct.[236] These measures create a fundamental tension with the doctrine of the rule of law, under which the law must apply equally to all persons, including the state and the individual officials through whom it acts.

580. Accordingly, it is incumbent on the proponents of the Bill to establish the necessity and proportionality of proposals to dispense with existing statutory authorisation requirements for the conferral of immunities and indemnities as part of controlled operations. As explained below, the Law Council considers that the essential requirements of necessity and proportionality not been substantiated in respect of the proposals in Schedule 4 to the Bill.

The identified 'problem' is capable of management under existing provisions

581. The Explanatory Memorandum states that the proposed amendments in Schedule 4 reflect the following circumstance:

---

[232] Bill, Schedule 4, items 1-3 (amending paragraph (2)(d) of ss 15GI, 15GQ and 15GV of the Crimes Act).

[233] Explanatory Memorandum, 6 at [27].

[234] Crimes Act, Division 3 of Part IAB (protection from criminal liability, and indemnity from civil liability).

[235] Ibid, subsection 15GA(2) (which requires a court, in considering whether to admit or exclude evidence, to disregard the fact that it was collected by a participant in a controlled operation, engaging in conduct that would otherwise be an offence but for the authorisation under that controlled operation).

[236] For an example of the usual discretion, which is modified by subsection 15FA(2) of the Crimes Act, see: *Ridgeway v The Queen* (1995) 184 CLR 19, in which the High Court overturned a conviction for drug offences, on the basis that investigating police had acted unlawfully to obtain the evidence (essentially, a covert 'sting' operation in which the AFP orchestrated the importation of a drug) with the result that the evidence was inadmissible because of that illegality. This case prompted the enactment of Part IAB of the Crimes Act.

> *While law enforcement will always ensure that illicit content is controlled, to the best of their ability, this provision acknowledges how easy data is to copy and disseminate, and that there may be limited guarantee that all illegal content (the illicit goods) will be under law enforcement's control at the end of an operation conducted online.*[237]

582. However, this statement appears to overlook that the requirement in existing paragraph (2)(d) of sections 15GI, 15GQ and 15GV is not an absolute requirement that law enforcement agencies must, invariably, have complete control over all 'illicit goods' (including data) at the conclusion of a controlled operation.

583. Rather, the requirement in the above provisions is that the agency must take all reasonable steps to ensure that it will be in a position to exercise control, to the maximum extent possible. The degree of control that is, or is not, possible in the circumstances is necessarily a question of fact for the issuing authority to determine at the time of considering a request to grant, vary or extend an authorisation for a controlled operation.

584. If law enforcement officers act in the manner described in the Explanatory Memorandum as standard practice—that is, to 'always ensure that illicit content is controlled to the best of their ability'[238]—then those actions would appear capable of being covered by the existing authorisation, variation and extension provisions in respect of exercising control over illicit goods 'to the maximum extent possible'.

585. There is nothing apparent in the ordinary meaning of the expression 'to the maximum extent possible' (as used in existing paragraph (2)(d) of sections 15GI, 15GQ and 15GV) that would seem to require a law enforcement agency to exercise a degree of control over data that is, in fact, impossible in the circumstances.

586. If the issuing authority is satisfied, on reasonable grounds, that it would not be possible for law enforcement to exercise any meaningful control over 'illicit goods' that consist of data that is obtained during a controlled operation conducted online (such as child pornography or other exploitation material), then it would nonetheless be legally possible for that issuing authority to grant the authorisation, variation or extension for the controlled operation. It is open to the AFP or ACIC as applicant for an authority to address this matter in their applications and supporting affidavits.

Relevant scrutiny principles articulated by the Richardson Review

587. As noted above, the Richardson Review commented, in strong terms, on the need to carefully interrogate assertions that existing legislation contains deficiencies, especially when the proposed statutory 'remedies' would repeal existing safeguards. The unclassified version of the review report stated:

> *Agencies had a tendency to suggest that legislative provisions presented barriers to their effective operation. Barriers agencies experienced were presented as unintended, rather than a consequence of deliberate design. On closer examination, it was often apparent that these barriers, to the extent that they in fact were barriers, were not due to legislation, but rather to culture, policy or practice. In other cases, a perception of the existence of barriers stemmed from an immature understanding of the principles governing the intelligence agencies.*

[237] Explanatory Memorandum, 181 at [1080].
[238] Ibid.

This lack of understanding led some agencies to suggest that legitimate safeguards should be removed … The ends do not always justify the means and the referenced legal requirements are important features designed, among other things, to protect individuals' rights … Likewise, what was argued to be an administrative burden was often a deliberately imposed safeguard. Alternatively, what was said to be an administrative burden was more properly characterised as a reasonable incident of the performance of functions in a liberal democracy. The term 'administrative burden' tends to be thrown around too loosely by agencies. Government should be wary of, and properly test, such claims.

Our laws are not constraints or barriers to operational effectiveness as they are sometimes perceived. Rather, they are guardians of valuable principles … Too often during the Review, proposals to 'clarify' or 'streamline' legislation amounted to no more than a bid to extend powers or functions. Government should be sceptical of calls for legislative clarity—very often such claims do not withstand even modest inquiry.[239]

588. For the reasons explained above, the Law Council considers that the measures in Schedule 4 to the Bill are an example of the circumstances identified by the Richardson Review, in which the perceived problem is not, in fact, a defect in the relevant provisions of Part IAB of the Crimes Act. Rather, based on the publicly available justification for the proposed amendments, the existing provisions of Part IAB of the Crimes Act are more accurately characterised as applying a carefully designed safeguard, which already takes account of the issues identified in the Explanatory Memorandum as the impetus for the proposed amendments.

Risks in granting an exemption for controlled operations conducted online

589. There are two significant risks in granting a wholesale exemption for online controlled operations from the requirements in paragraph (2)(d) of sections 15GI, 15GQ and 15GV, as explained below.

Removal of statutory obligations even where it is possible to exercise control

590. First, there may be circumstances in which it is possible for a law enforcement agency to exercise a meaningful degree of control over illicit data that is accessed or disseminated as part of a controlled operation. The proposed amendments would have the effect of relieving the agency of the legal requirement to do so in these circumstances, as a precondition to the issuance of the authorisation for the controlled operation.

591. The extrinsic materials to the Bill have not excluded the possibility that there may presently be technical solutions that could be deployed (for example, the application of access controls to prevent the copying or dissemination of data, the seizure of computers or data storage devices, takedown notices or voluntary cooperation of communications providers in relation to illicit content hosted on their platforms, and the exercise of the proposed data disruption powers). In addition, it is possible that new solutions could be developed in the future, as technology advances.

592. The Law Council is therefore concerned that the wholesale exclusion proposed in Schedule 4 to the Bill would remove any statutory obligation, and potentially a strong incentive, to use existing capabilities and powers, or pro-actively seek out or

[239] Richardson Review, *Unclassified Report, Volume 1* (December 2019), 34-35.

develop new ones, to exercise control over harmful or illicit content that is accessed or disseminated as part of an online controlled operation.

593. In other words, if the measures in Schedule 4 to the Bill are passed, the law governing the conduct of online controlled operations may be 'frozen in time' to reflect present technical limitations, or perceived limitations, on the ability of law enforcement officers to exercise meaningful control over illicit data that is accessed or disseminated as part of a controlled operation.

594. Just as there is a legitimate objective in ensuring that laws conferring security and law enforcement-related powers are keeping pace with technological developments, and are drafted to be as 'technology neutral' as possible, it is equally important that such laws do not confer effective immunities from legal liability in a manner that risks entrenching present limitations in capability.

Unintended consequences

595. The limited justification provided in the Explanatory Memorandum appears to contemplate circumstances in which harmful content, such as child abuse material, is accessed or disseminated as part of a controlled operation conducted online.

596. However, a controlled operation that is conducted online could authorise an extremely broad range of otherwise unlawful activities. For example, it would be technically possible for a controlled operation carried out online to disseminate a computer virus, or other malicious data that would otherwise weaken or remove protection applied to data held on a computer, which could otherwise constitute a computer offence in Part 10.7 of the Criminal Code. (This is provided that the relevant act is not conduct for which a computer access warrant is required, as this is excluded from the immunities conferred on participants in controlled operations under section 15HC of the Crimes Act.)

597. In these circumstances, the Law Council considers it appropriate that law enforcement agencies should be required to satisfy the issuing authority that they will be able to control that virus or malicious data, to the maximum extent possible, at the conclusion of the controlled operation. This will necessarily require the presentation of evidence about available technical capabilities to control that data, and the likely feasibility and effectiveness of their deployment.

598. If there are genuinely no reliable capabilities available, or if their deployment would be disproportionately onerous on the law enforcement agency, then the approving authority could take these matters into consideration in deciding whether to grant the authority. In other words, if there are genuinely no reasonable means available to a law enforcement agency to control illicit data, then the duty in existing paragraph (2)(d) of sections 15GI, 15GQ and 15GV to take all reasonable steps to exert control is 'reduced, in practical terms, to nothingness'.[240]

[240] *Leghaei v Director General of Security* [2005] FCA 1576 (10 November 2005) at [83] (Madgwick J). The quoted expression was the judicial description of the content of a duty to accord a person procedural fairness in the making of an administrative decision (a security assessment) by disclosing relevant information, which was highly classified. The quoted expression used by the trial judge in this case is also apt to describe other scenarios in which the substance of a legal duty can be effectively 'hollowed out' or negated, because of the factual circumstances involved in a particular case.

Recommendation 56—omission of Schedule 4 from the Bill

- **Schedule 4 should be omitted from the Bill, in recognition that the issues that have given rise to the perceived need for the amendments are, in fact, capable of being managed under the existing provisions governing the authorisation of controlled operations.**

Ambiguity in the acts excluded from controlled operations

599. Section 15HC of the Crimes Act provides that the criminal immunities and civil indemnities under Part IAB do not apply to certain conduct. This is generally conduct for which a law enforcement agency would require a warrant or another form of statutory authorisation under a separate law. The following actions are excluded:

    (a) arrest or detention of individuals;

    (b) searches of individuals;

    (c) entry onto, or searches or inspection of, premises;

    (d) searches, inspections or seizures of other property;

    (e) forensic procedure;

    (f) electronic surveillance devices or telecommunications interception;

    (g) identification procedures;

    (h) the acquisition or use of assumed identities; or

    (i) any other matter concerning powers of criminal investigation.

600. The Law Council is concerned that acts done under data disruption warrants and network activity warrants (or emergency authorisations of those powers) are not clearly covered by the list of exclusions in section 15HC of the Crimes Act.

601. In particular, such actions are not strictly matters concerning 'criminal investigations' for the purpose of existing paragraph (i). Rather, the proposed data disruption powers are directed principally to covertly frustrating, rather than investigating and enforcing, the commission of an offence. Additionally, the proposed network activity powers are directed to the collection of criminal intelligence about organised crime networks, rather than the investigation and enforcement of specific offences.

602. The highly intrusive and serious consequences of controlled operations makes it necessary to have complete clarity about the excluded conduct, which should be made explicit on the face of section 15HC of the Crimes Act. The provision needs to speak clearly and directly to the law enforcement officers who request and execute controlled operation authorities, as well as issuing authorities, civilian participants, and persons who are adversely affected by criminal or tortious conduct that is carried out as part of a controlled operation. Every effort should be made to remove sources of legal ambiguity or practical confusion in the scope and limits of powers to authorise and conduct controlled operations.

603. Accordingly, the Law Council recommends that section 15HC should be amended to expressly exclude conduct that would require authorisation under a data disruption or network activity warrant, or an emergency authorisation for such activities.

Recommendation 57—amendment to section 15HC of the Crimes Act

- **To avoid any doubt or uncertainty, section 15HC of the Crimes Act should be amended to provide expressly that a controlled operation cannot authorise, or confer criminal immunity or civil indemnity for, activities in respect of which a data disruption warrant, or a network activity warrant is required under the SDA (or an emergency authorisation for these activities).**