Australian Government
Department of Home Affairs

Department of Home Affairs supplementary submission to the review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

23 April 2021

Table of Contents

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to make a supplementary submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill). As requested by the Committee, the submission responds to questions on notice from the Committee following the public hearing for this review held on 10 March 2021 (see **Attachment A** and **Attachment B**). This submission includes input from the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC), the Australian Signals Directorate (ASD), the Attorney-General's Department, and the Department of Infrastructure, Transport, Regional Development and Communications.

Responses to recommendations made by the Law Council of Australia

2. The below provides the Department's response to recommendations made by the Law Council of Australia (Law Council) in its submission to the Committee's review. A full list of recommendations is provided at **Attachment A**.

Data disruption warrants (Schedule 1)

Recommendation 1 – implementation of Richardson Review recommendations regarding disruption

3. The Government agrees that the AFP (and the ACIC) should fully utilise existing powers to combat cybercrime. However, those powers are increasingly ineffective against large-scale incidents of cyber-enabled crime. The Government considers that legislative reform is necessary to enhance the ability of the AFP and ACIC to discover and disrupt serious criminality online—in the first instance through the powers in this Bill, including data disruption warrants. Data disruption warrants were developed after careful consideration of the potential practical and principled issues in relation to disruption as identified by the Comprehensive review of the legal framework of the National Intelligence Community (Richardson Review).

4. The Home Affairs principal submission to the Committee's review further outlines the findings of the Richardson Review and the Government response as they relate to this Bill, with a particular focus on disruption.[1] Further detail about the current threat environment, and why the three new powers in the Bill are needed in addition to the existing framework, is also contained in the Home Affairs principal submission[2] and the AFP principal submission.[3]

5. The Law Council's alternative recommendation that data disruption warrants should be authorised only by judicial officers, and not Administrative Appeals Tribunal (AAT) members, is addressed in response to **Recommendation 5**.

Recommendation 2 – persons who may apply for data disruption warrants

All warrant applications are subject to independent scrutiny

6. At the public hearing on 10 March 2021, the AFP and the ACIC gave evidence that, for operational reasons, it is important that persons with relevant knowledge (rather than necessarily those of senior

[1] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p 11–12.
[2] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, (Submission 9),* p. 5.
[3] *AFP submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, (Submission 6),* p. 5-8

rank) should apply for warrants, and that there are internal procedural arrangements which ensure that decisions to apply for warrants are approved by senior officers (described below). Most importantly, all warrant applications—and the decisions to authorise certain activities under warrant—are subject to independent scrutiny by an AAT member or judicial officer.[4]

7. Issuing authorities must afford the same level of scrutiny and consideration to all warrant applications regardless of the level of officer or role of the person applying for the warrant. Oversight of decisions to apply for warrants by judicial officers and AAT members (and magistrates in the case of account takeover warrants) provides for independent review of agencies' decisions to apply for warrants and satisfaction of reasonableness and proportionality.

Persons with relevant knowledge, rather than senior rank, should apply for warrants

8. As with existing warrants in the *Surveillance Devices Act 2004* (Surveillance Devices Act), data disruption warrants and account takeover warrants can be applied for by law enforcement officers of the AFP and the ACIC. The definition of 'law enforcement officer' in existing section 6A of the Surveillance Devices Act includes all employees of, and secondees to, the AFP and the ACIC. The flexibility in who (within those agencies) may apply for such warrants is necessary to address operational needs; noting that in practice the making of the application can only be done after a decision has been made—at appropriately senior levels—within the AFP and the ACIC to apply for a warrant.

9. From an operational perspective, the AFP advises that it is strongly preferable that warrant applications are not restricted to only 'senior' or commissioned officers. It is important to ensure that, in all circumstances, the most appropriate person is able to apply for a warrant. This will be the person who has the relevant detailed knowledge about the investigation or operation should the issuing authority have questions in the course of considering the application. This will not necessarily be an officer who holds a senior rank in his or her agency.

10. Another person may also apply for a data disruption warrant or account takeover warrant, but this may only be done on the law enforcement officer's behalf. This is intended to allow for legal practitioners within agencies and unsworn officers to physically make the application for warrants, where it is appropriate to do so, on behalf of the law enforcement officer. This ensures that an investigation can proceed efficiently regardless of circumstance which may require sworn resources to be re-allocated. For example, the ACIC uses the ability for another person to apply on behalf of the law enforcement officer for practical purposes, such as when the law enforcement officer is on leave or is unavailable due to competing priorities.

Internal policies and procedures for the application of warrants

11. The person physically applying for the warrant is not necessarily the person who makes the decision that an application for a warrant should be made. The AFP and the ACIC have internal policies and procedures governing the process for deciding to make an application for warrants under the Surveillance Devices Act, as well as policies and procedures regarding the application process itself.

12. AFP governance requires warrants to be reviewed by a more senior AFP member and, depending on the type of warrant, be accompanied by a technical capability or execution plan. Similarly, the ACIC has advised that warrants are applied for by the principal law enforcement officer for a given operation, following approval by the relevant team leaders and the state investigations manager.

13. The AFP has mandatory training requirements to ensure all AFP members who are eligible to apply for warrants, or authorise the use of powers, are familiar with their legislative obligations. This training provides all information required for members to understand the powers available under legislation, their statutory obligations and threshold requirements, any reporting obligations and oversight, the importance of legislative compliance and adverse consequences for non-compliance, and how to find

[4] Mr Reece Kershaw APM (AFP Commissioner) and Mr Michael Phelan APM (ACIC CEO) *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 58–61

assistance and resources to meet their obligations. The AFP's training is regularly inspected by the Ombudsman.

14. The ACIC advises that to achieve the highest standard of compliance with reporting, accountability and oversight measures associated with the Surveillance Devices Act and the *Telecommunications Interception and Access Act 1979* (TIA Act) (and any other legislation providing the ACIC with similar powers), the agency has an Excellence in Compliance Strategy and training scheme. This consists of mandatory annual training and assessment requirements for staff who will be applicants for warrants and who need to access any information captured by a surveillance device or a telecommunications intercept or authorisation.

15. Data disruption warrants and account takeover warrants are subject to oversight by the Commonwealth Ombudsman, who is empowered to inspect records to determine legislative compliance, including warrant applications.

Recommendation 3 – 'relevant offences' for data disruption warrants

A three-year offence threshold

16. As noted in the Home Affairs principal submission, the warrants in the Bill are subject to strict thresholds that ensure that they may only be sought where reasonable and proportionate. Each power has been designed to align with the legislative framework in which it sits, and, as much as possible, to align with other powers that agencies are likely to use in conjunction with these new warrants. This is to reflect the fact that agencies require and use a suite of powers to tackle online crimes that are complex, evolving, and often occur on multiple devices and across multiple jurisdictions.[5] Each of the powers must be sought in respect of 'relevant offences', that is, generally offences punishable by a maximum term of imprisonment of three years or more.

17. The definition of 'relevant offence' is not static and will expand when Parliament enacts a new offence that meets the three-year threshold, or increases the maximum penalty for an existing offence which would bring it within this offence threshold. Given the speed with which technology and digital crimes are evolving, listing specific Commonwealth and State and Territory offences as 'relevant offences' would require frequent legislative amendment and would cause the threshold to be out of date as State and Territory legislative changes are made.

Prescribing additional offences by regulation

18. As noted in the Law Council's submission, a 'relevant offence' in the Surveillance Devices Act may also include offences that are prescribed by regulations. Under existing section 66 of the Surveillance Devices Act, the Governor-General may make regulations prescribing matters required or permitted by the Surveillance Devices Act or necessary or convenient to be prescribed for carrying out or giving effect to that Act. The ability to prescribe offences by regulation would be an important option, subject to Parliamentary oversight, for ensuring that the definition of relevant offence in the Surveillance Devices Act keeps pace with changes in technologies and evolutions in criminal behaviour. There are no regulations that have been made prescribing additional offences in the Surveillance Devices Act, since the Act was introduced in 2004. If additional offences were to be prescribed, the making of the regulations would be subject to appropriate Parliamentary oversight and scrutiny, and to motions of disallowance.

Raising the offence threshold to seven year offences

19. The Law Council's proposal to raise the offence threshold to an offence punishable by a maximum penalty equivalent to the threshold for telecommunications interception warrants in paragraph 5D(2)(a) of the TIA Act (generally seven years' imprisonment or more) relates to the seven-year offence threshold outlined at paragraph 5D(2)(a) and not the range of ad-hoc exceptions for offences with a range of lower penalties.

---

[5] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p. 18.

20. Raising the offence threshold to seven-year offences would result in a number of serious offences not being captured by the warrants. This is despite those offences involving serious and abhorrent conduct, for example:

    a. using a carriage service to menace, harass or cause offence (section 474.17 of the *Criminal Code Act 1995* (Criminal Code)). This offence can be extremely serious. For example, prosecutions under section 474.17 have included online grooming and procuring and the non-consensual sharing of intimate images.[6]

    b. associating with a terrorist organisation (section 102.8 of the Criminal Code)

    c. failing to report child sexual abuse offences (section 273B.5 of the Criminal Code), and

    d. conduct by Commonwealth officers causing harm to Australian interests (section 122.2 of the Criminal Code).

21. Three-year offences are also often conducted alongside other serious offences attracting higher penalties. As raised by the AFP Commissioner at the public hearing, organised crime groups (such as outlaw motorcycle gangs) are often engaged in a range of criminal offending from lower-level offences such as supplying vehicles to serious offences such as trafficking illicit drugs and money laundering.[7] At the public hearing, Dr Zirnsak, representing the Uniting Church in Australia, used the example of an individual setting up a shell company for the purposes of financing terrorism to demonstrate that '[a]n investigation of what might be a more minor offence initially might unravel a much larger operation.'[8] The ability to target the offences at the lower end of that spectrum under these warrants will assist the AFP and the ACIC in dismantling criminal networks.

22. The Richardson Review noted that raising the offence threshold for electronic surveillance warrants to apply to seven-year offences would have 'no particular principled basis, and would amount to simply adopting a 'highest common denominator' approach.'[9] The Department notes that raising the offence thresholds for the warrants in this Bill to five years—as recommended by the Richardson Review for electronic surveillance powers—would place data disruption warrants, network activity warrants and account takeover warrants out of step with the current electronic surveillance framework in which they were designed to fit. The Department is considering how to implement the Richardson Review's recommendation for broader electronic surveillance reform, as accepted by Government, including the recommendation regarding the five year offence threshold (with exceptions) for electronic surveillance warrants (recommendations 87 and 89).[10]

Recommendation 4 – stronger criteria directed to necessity and proportionality

23. In order to issue a data disruption warrant, the eligible judge or AAT member must be satisfied that, amongst other things, the disruption of data authorised by the warrant is justifiable and proportionate with regard to the offences targeted. A threshold of justifiable and proportionate has been set rather than 'reasonably necessary' due to the nature of the criminal activity targeted by data disruption warrants, that is, serious crimes perpetrated on the dark web or through the use of anonymising technologies. As a result of the use of these obfuscating tools, there is unlikely to be sufficient

[6] Commonwealth Director of Public Prosecutions (CDPP), *News and Media Releases: Online grooming and blackmail of girls lands man in goal*, 17 November 2017, https://www.cdpp.gov.au/news/online-grooming-and-blackmail-girls-lands-man-gaol; Commonwealth Director of Public Prosecutions (CDPP), *Crimes We Prosecute: Cyberbullying and Threats*, https://www.cdpp.gov.au/crimes-we-prosecute/cyberbullying-and-threats
[7] Mr Reece Kershaw APM (AFP Commissioner) *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 52
[8] Dr Marcus Zirnsak, Uniting Church in Australia Synod of Victoria and Tasmania, *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 19-20
[9] Mr Dennis Richardson AC, *Comprehensive review of the legal framework governing the National Intelligence Community* (2019) Volume 2, p. 309. para. 28.102.
[10] Attorney-General's Department, *Government response to the Comprehensive Review of the Legal Framework of the National Intelligence Community by Mr Dennis Richardson AC,* (2019) p. 26–27.

information at the time of application that would satisfy the issuing authority that the proposed data disruption activity is reasonably necessary.

24. It may not always be possible, at the time of applying for the warrant, for an agency to estimate the full extent to which activity required to undertake data disruption is likely to have an impact on third parties. In light of this, rather than providing for an express privacy consideration the Bill contains a mandatory condition that the issue of a data disruption warrant be justified and proportionate having regard to the offences targeted.

25. The Department has provided further explanations of the criteria for the issuing of a data disruption warrant in the Explanatory Memorandum[11], the Ministerial response to the Senate Standing Committee for the Scrutiny of Bills[12] and the Ministerial response to the Parliamentary Joint Committee on Human Rights.[13]

26. Noting the issues raised by the Law Council, the Department will consider the implications of an expansion to the mandatory considerations for the issue of data disruption warrants to explicitly include consideration of the extent to which the execution of the warrant is likely to result in the disruption of data of persons who are lawfully using a computer. This would be similar to the consideration for the issue of network activity warrants at paragraph 27KM(2)(f).

Recommendation 5 – superior court judges as sole issuing authorities

27. In the Bill, the power to issue data disruption warrants and network activity warrants is conferred on an eligible Judge or a nominated AAT member. Warrant applications to Judges and AAT members are subject to the same requirements and must stand up to the same level of scrutiny. Independent scrutiny of warrant applications by eligible Judges or nominated AAT members is an important mechanism in ensuring that warrants are only issued when reasonable and proportionate, and that the powers are consistent with Australia's international human rights law obligations.

28. The Department refers to the Ministerial responses to the Senate Standing Committee for the Scrutiny of Bills and Parliamentary Joint Committee on Human Rights in relation to this issue. Those responses explain that AAT members have the experience and skills necessary to issue data disruption warrants and network activity warrants, and that AAT members are independent decision makers equipped to undertake this role.[14]

29. The Ombudsman provided evidence to the Committee that it has not yet identified any differentiation in terms of the outcomes from their inspections in relation to warrants and authorisations that were issued by a judge versus those that were issued by a member of the AAT. The Ombudsman also noted that his Office had not seen anything, one way or the other, that illuminated whether there was any correlation in the difference in outcome if the authorising officer is an AAT member or a judicial officer.[15] The Ombudsman's Office does not consider the merits of a decision by a judicial officer or an AAT member to issue a warrant. When discussing the appropriate issuing authority for account takeover warrants, the Ombudsman also noted that both judges and AAT members are well equipped, accustomed to, and have more background experience in issuing warrants in the covert space when compared to magistrates who tend to issue overt warrant types.[16]

---

[11] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 30, para. 69.
[12] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 124.
[13] *Ministerial Response to the Parliamentary Joint Committee on Human Rights – Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Report 3 (2021) p. 73.
[14] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 121-122; *Ministerial Response to the Parliamentary Joint Committee on Human Rights – Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Report 3 (2021) p. 70-72.
[15] Mr Michael Manthorpe PSM (Commonwealth Ombudsman, Office of the Commonwealth Ombudsman) *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 43.
[16] Mr Michael Manthorpe PSM (Commonwealth Ombudsman, Office of the Commonwealth Ombudsman) *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 39.

Richardson Review recommendations on judicially authorised disruption powers

30. The Law Council cites the Richardson Review's findings in relation to judicial authorisation of disruption activity involving damage to or destruction of property.[17] However, the proposed data disruption warrant is focused on disrupting data only with strong safeguards that expressly prohibit causing loss or damage to data that is not justified and proportionate, and prohibit the causing of permanent loss of money, digital currency or property other than data.

Review of administrative decisions

31. Under this Bill, Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of section 39B of the *Judiciary Act 1903*, or under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act).

Recommendation 6 – an 'Investigatory Powers Division' of the AAT to issue data disruption warrants

32. For the reasons outlined in response to the **Recommendation 5** above, the Department considers it appropriate for data disruption warrants and network activity warrants to be issued by eligible Judges and nominated AAT members. In response to the Law Council's recommendation in relation to the establishment of an Investigatory Powers Division of the AAT, the Department refers to its previous response to the Independent National Security Legislation Monitor (INSLM) review in its supplementary submission to the Committee's third review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act), and in particular the significant practical issues for the AAT that an Investigatory Powers Division would create.[18]

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

33. The Department does not consider that a regime for public interest advocates to act as contradictors in applications for data disruption warrants is necessary, or that such a regime would be effective in protecting the range of public interests that may be relevant.

34. Beyond considering the right to privacy, it is unclear what the role of the proposed public interest advocate would be. At the public hearing, Dr Zirnsak representing the Uniting Church in Australia, made the point that there are other forms of public interest, such as the interests of the victims of sexual abuse that are relevant to the existence and exercise of powers for law enforcement to combat serious crime.[19] Adequate and appropriate protection of privacy is clearly a public interest matter—but so too is the prevention of crime, and the investigation into and prosecution of serious offences, including human rights abuses.

35. As noted in the Ministerial response to the Parliamentary Joint Committee on Human Rights, the warrants in the Bill are supported by a range of safeguards, stringent thresholds and oversight arrangements to protect the rights of an affected person and provide for independent scrutiny and review of decisions relating to the warrants.[20] These measures will mitigate any need for public interest advocates to act as contradictors for all warrants.

---

[17] Mr Dennis Richardson AC, *Comprehensive review of the legal framework governing the National Intelligence Community* (2019) Volume 3, p. 220-221.
[18] Department of Home Affairs, *Supplementary submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Submission 16.2) (2020) p. 6.
[19] Dr Marcus Zirnsak, Uniting Church in Australia Synod of Victoria and Tasmania, *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 20
[20] *Ministerial Response to the Parliamentary Joint Committee on Human Rights – Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Report 3 (2021) p.79.

36. The Government agreed to the recommendation made by the Committee for the expansion of Public Interest Advocates following its inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (the press freedoms inquiry). However, this is more limited in scope than the recommendation made by the Law Council in relation to this Bill. In response to the press freedoms inquiry, the Government agreed to the expanded role of Public Interest Advocates in relation to overt and covert warrants, when the warrant is sought for a journalist or media organisation, and where the warrant is related to the investigation of an offence in relation to an unauthorised disclosure of Commonwealth government information or contravention of a Commonwealth secrecy offence.[21]

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

37. Noting the observation made by the Richardson Review that the concept of disruption is 'nebulous,' the Law Council has stated that the Bill does not include a definition of 'disruption'. The Department does not agree with the Law Council's assessment. The Bill includes a definition of 'disrupting data' in subsection 6(1) of the Surveillance Devices Act (item 8 of Schedule 1 of the Bill). This definition provides that disrupting data means adding, copying, deleting or altering data held in a computer in relation to data disruption warrants and emergency authorisations for disruption of data. There are strong safeguards that expressly prohibit causing loss or damage to data that is not justifiable and proportionate or causing any permanent loss of money, digital currency or property other than data under a data disruption warrant or emergency authorisation.

38. The Bill does not define the term 'frustrate' in relation to the commission of an offence. Instead, the term takes on its ordinary meaning.[22] The deliberate decision was made not to define what 'frustrate' means beyond the ordinary meaning, which provides sufficient clarity while also providing the operational flexibility the AFP and ACIC require to make effective use of data disruption warrants. Data disruption action taken by the AFP or the ACIC may 'frustrate' criminal offending in more than one way, and it may not be possible to specify the particular nature of the frustration at the time of applying for the warrant. For example, the action of removing illegal material from a website may frustrate criminal offending by preventing a person from selling that material, preventing a person from accessing that material, reducing the risk of harm to victims of that material, damaging a criminal organisation's reputation for providing that material, eventually having an impact on the production of such material, or having other flow-on effects.

Law Council alternative option to provide further information in warrant applications

39. The Department considers the criteria for applying for a data disruption warrant to be satisfactory.

40. Applications for data disruption warrants will need to provide as much information as necessary for the issuing authority to be satisfied that there are reasonable grounds that:

    a. the disruption of data is likely to substantially assist in frustrating the commission of relevant offences, and

    b. the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences targeted.

41. Consideration of these matters, and satisfaction of the issuing criteria, will necessarily require warrant applications to set out important facts and grounds. This would include the data disruption activity proposed to be carried out under the warrant, the anticipated impacts of the proposed activity on the commission of the offences, and the likelihood that the proposed activity will assist in frustrating the commission of those offences. However, it will not always be possible for an applicant to anticipate all of the impacts of data disruption, or all of the offences that that disruption will or may frustrate. For example, it will often be unknown exactly who would have committed a further offence if the disruption

[21] *Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report: Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (2020) p. 4.
[22] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 27, para. 50.

activity had not taken place. In addition, while subsection 27KC(2) sets out mandatory considerations to which an issuing authority must have regard in assessing warrant applications, this does not preclude the consideration of any other things that the issuing authority may wish to take into account.

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

Prohibition on causing loss or damage to third parties

42. Prohibiting the AFP and the ACIC from causing any material loss or damage to third party users under any circumstances would narrow data disruption warrants to the point where they cannot be used to effectively frustrate criminal offending. There may be circumstances in which it would be justified and proportionate to cause loss or damage to the data of third parties. For example, it may be justified and proportionate for the AFP or the ACIC to shut down a particular online site hosting the live-streaming of child abuse despite the owner or administrator of that site not necessarily being suspected of this type of criminality. It may also be justified or proportionate where a third-party's computer or server is being used to host data which is facilitating serious offences (not just limited to child abuse material) and it is impossible to remove that data using other means.

43. Introducing an absolute prohibition on causing material loss or damage to persons who are not suspects or persons of interest makes the situations above impractical to target with a data disruption warrant, and will encourage criminals to adapt their methodologies to respond to this gap in law enforcement's coverage. Due to the sophistication of modern computer systems and networks, it will be difficult if not impossible to make targeted changes that are guaranteed to impact only intended computers. For this reason, a proportionality requirement has been inserted into the Bill, in addition to the prohibition on causing damage to data unless that damage is justified and proportionate.

44. The Bill also includes statutory conditions which provide that if loss or damage to data occurs during the execution of a warrant, the damage must be justified and proportionate. The statutory conditions do not restrict the issuing authority's ability to prescribe additional conditions under those provisions, to which the execution of the warrant would then also be subject.[23]

45. Warrants must not be executed in a manner that causes a person to suffer a permanent loss of money, digital currency or property (other than data). This is intended for an abundance of clarity about the scope of the warrants. Interference with a person's money, digital currency or property that is not data is not the intended purpose of either of these warrants.

46. Importantly, as discussed above in response to **Recommendation 5**, an affected person has an avenue to challenge decisions made in regards to warrants through judicial review. Australian courts will retain their jurisdiction to review administrative decisions through the original jurisdiction of the High Court and in the Federal Court of Australia by operation of section 39B of the *Judiciary Act 1903*, or under the ADJR Act. In addition, where a person suffers loss of, or serious damage to, property or personal injury as a result of the execution of a warrant (or emergency authorisation), the Commonwealth is liable to compensate that person.

Law Council alternative option – raising the threshold for causing loss or damage, limiting actions and additional requirements for warrant applications

47. As outlined above in response to **Recommendation 4**, the Department notes that consideration could be given to including explicit consideration of the extent to which the execution of the warrant is likely to result in the disruption of data of persons who are lawfully using a computer. This would be similar to the consideration for the issue of network activity warrants at paragraph 27KM(2)(f). Consideration of this matter, in addition to the current mandatory considerations for the issue of data disruption warrants, would clarify that data disruption warrants cannot be issued without consideration to the likely impact of the execution of the warrant on third parties.

[23] *Ministerial Response to the Parliamentary Joint Committee on Human Rights – Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Report 3 (2021) p. 75.

48. In its submission, the Law Council proposed that the ability to cause loss or damage under a data disruption warrant should be limited to data disruption activities alone, and not also 'any thing' authorised by the warrant (under subsection 27KE(2)). However, the Department notes that the specified things listed at subsection 27KE(2) are limited only to things that are necessary to execute the data disruption warrant (i.e. enable the disruption of data held in a computer). In some cases it will be impracticable, or even impossible, to make a distinction between the data disruption activity and the things authorised under the warrant that are necessary to enable the disruption of data held in a computer. For this reason, it is important that the ability to cause material loss or damage is not limited to data disruption activities alone so as not to undermine the overall effectiveness of the warrant.

Law Council alternative option – requirement to notify Commonwealth Ombudsman of loss or damage caused and additional annual reporting requirements

49. The Department notes that the AFP and the ACIC are required to notify the Ombudsman about the exercise of actions undertaken for the purposes of frustrating criminal activity under a data disruption warrant. This will necessarily involve providing notice of any actions undertaken that have caused material loss or damage to third parties. This notification requirement supports the Ombudsman's role in inspecting agencies' records to determine the extent of their compliance with the requirements for data disruption warrants, including the limitations on causing material loss or damage to third parties at subsection 27KE(7).

50. From a practical perspective, the Department notes that the Ombudsman conducts retrospective inspections. For example, in the 2020–21 year, the Ombudsman inspects warrants or authorisations that expired in the 2019–20 year. The legislation does not require the Ombudsman to do this, but there is less risk of potentially compromising an ongoing investigation with this approach. Accordingly, while the Ombudsman may be notified about certain things occurring, it is unlikely, in practice, that the Ombudsman would inspect records relating to contemporaneous investigations.

51. The Law Council's recommendation to expand the notification requirements for data disruption warrants is addressed below in response to **Recommendation 20**. The Law Council's recommendation to expand the annual reporting requirements for data disruption warrants to include information about loss or damage caused to third parties is addressed below in response to **Recommendation 26**.

Law Council alternative option – consequential amendments to the Criminal Code and Intelligence Services Act in relation to ASD

52. ASD staff members or agents are only able to avail themselves of limitation of liability provisions in Division 476 of the Criminal Code and section 14 of the *Intelligence Services Act 2001* (Intelligence Services Act) to the extent that they are acting in the proper performance of ASD's functions. In relation to supporting to the AFP or the ACIC, the effect of section 7(1)(e) of the Intelligence Services Act (ASD's assistance function) is that ASD staff can properly do nothing more than what the AFP or the ACIC have the power to do themselves. Were an ASD staff member to do something beyond what the AFP or the ACIC was empowered to do in the course of assisting either agency, this would not be in the course of the proper execution of ASD's functions and the liability limitation provision would be no answer to a criminal or civil claim.

Recommendation 10 – scope of telecommunications interception power

53. Data disruption warrants and network activity warrants, like existing computer access warrants, permit the interception of a communication passing over a telecommunications system only if doing so is for the purposes of executing the warrant (see Home Affairs principal submission[24]). Computer access capabilities do not work in a vacuum and require some degree of knowledge and interaction with the telecommunications system before execution. As a result, it will often be necessary for law enforcement agencies to intercept communications to make access to or disruption of data practicable or technically

[24] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p. 24

possible, and to be able to maintain the necessary covert nature required to ensure these activities are both possible and effective.

54. Importantly, data disruption warrants and network activity warrants cannot authorise the collection of evidence or intelligence by interception. If the AFP or the ACIC require interception to do anything more than facilitate execution of a data disruption or network activity warrant—for example, if the AFP or the ACIC want to gather evidence by interception—those agencies must seek a separate interception warrant from an eligible issuing authority under the TIA Act.

55. Without the ability to intercept communications under a data disruption warrant or network activity warrant, it will be difficult to implement what is proposed under the warrant. In particular, interception must be available for the purpose of entering or existing premises, as it can prove essential in preventing the target of the warrant from being alerted through an electronic security system (such as, an alarm or camera) that they are under law enforcement surveillance. Interception could also be essential to alerting the AFP or the ACIC where a target could become aware of an investigation against them through, for example, an automated email being sent when an account or computer is accessed from a new or unknown IP address, or through any other automated notification when new or irregular activity occurs with an online account.

56. The Law Council has also expressed a concern about the subsequent use and disclosure under the TIA Act of interception information obtained under a data disruption warrant. The exceptions to the prohibition on use and disclosure of information intercepted under a data disruption warrant are essential, and only used in extreme circumstances, for example if the information relates to activities that present a significant risk to a person's safety, or activities that are likely to be a threat to security.

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

Power to use force under warrant

57. Similar to existing computer access warrants for law enforcement, the proposed data disruption warrants and network activity warrants authorise officers of the AFP and the ACIC to use force against persons or things only where necessary and reasonable to do the things specified in the warrant.

58. The ability to use force under warrant is required due to the eventualities that officers may face while executing a warrant. For example, it may be necessary to use force against a door or a cabinet lock to access a thing on the premises or to use force to install or remove a computer from a premises. In the case of force against a person, its use is constrained on the face of the legislation to circumstances where force is required to execute the warrant—for example, if a person is in physically preventing an officer from accessing a computer or other thing that needs to be used for the purposes of obtaining access to the relevant data under warrant. Use of force may also be necessary to ensure the safety of AFP and ACIC officers in the event a person acts aggressively.

59. The need to use force will not be limited to entry to or exit from a premises. For example, devices that are permitted to be removed from premises may require force to be exerted to remove storage or other items to enable the extraction of relevant data. This may occur after or at any time following an entry to a premises and the removal of those devices.

Decisions should not be made at the discretion of issuing authorities

60. The absence of a power to use reasonable and necessary force could potentially lead to civil action or criminal charges should an officer of the AFP or the ACIC do acts or things against a person proportionate to what is required by warrant. Limiting use of force to that authorised by the discretion of the issuing officer may not be workable, noting it may not be possible to foresee or plan for all situations in which use of force may be required over the life of the warrant, due to changing operational circumstances.

Power to use force should not be limited to only police officers

61. The ability to use force under a data disruption warrant or network activity warrant should also extend beyond police officers, noting that specialist skills (such as those of a locksmith) may be required to force a door, safe or other container.

AFP internal governance arrangements regarding use of force

62. In addition to the protections built into the Bill, general use of force principles for the AFP will apply, as overseen and regulated by a variety of internal governance arrangements—for example, the AFP Commissioner's Order 3, which sets out the policy and procedures in relation to operational safety and use of force.[25] These governance instruments form part of the AFP's professional standards framework, and any breach is taken very seriously within the AFP.

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

63. The Bill provides that the AFP and the ACIC will be permitted to temporarily remove a computer or other thing from premises for the purposes of executing a data disruption warrant or network activity warrant. A computer may need to be removed from premises to allow the AFP or the ACIC to analyse, or obtain access to, the data held on it, using specialised equipment located offsite. The category of other things that may be removed is limited to things that are, in some way, needed to execute the warrant. This will often be data storage devices or other peripheral items for the operation of a computer but may also include, for example, a piece of paper with a password written on it or a computer manual. It could also include a safe or vehicle believed to contain such information that is otherwise unable to be accessed during the entry to a premises. The computer or other thing that is removed from the premises must be returned once it is no longer required.

Recommendation 13 – statutory safeguards for post-warrant concealment powers

64. The Bill makes provision for the AFP and the ACIC to perform activities to conceal any thing done under a data disruption warrant, a network activity warrant or an account takeover warrant. Concealment activities may be carried out while the warrant is in force, within 28 days after the warrant is in force, or at the earliest time after that period at which it is reasonably practicable. A period of longer than 28 days would be required, for example, where a computer being accessed under a data disruption warrant or network activity warrant is moved by the target and the agency must wait for it to be physically relocated and recovered.

65. As noted in the Ministerial response to the Senate Standing Committee for the Scrutiny of Bills, making provision for concealment activities allows an agency to prevent targets learning that they are under investigation.[26] Without provision for concealment, activity under these warrants is likely to alter data, or leave traces of activity, on an electronic device or online account. This may allow targets to recognise the lawful intrusion and change the way they communicate for the purposes of evading detection. Recognition may lead to targets reverse engineering police capabilities and methodology, leading to targets avoiding the use of certain technologies or undertaking counter-surveillance activities.

66. Accordingly, the concealment of the execution of the warrants in the Bill is vital to the effective exercise of powers and maintaining the covert nature of the investigation or operation. In particular, it is appropriate that concealment activities can occur without additional external approval as the concealment activities are incidental to the granting of the original warrant. The precise nature of and opportunity for concealment activity may be difficult to predetermine. Concealment activity may need to occur with the utmost urgency to prevent detection of sensitive policing technologies or methodologies. This means that it may not be practicable to obtain external approval additional to that obtained through the original warrant.

67. Concealment measures are subject to limitations, safeguards and oversight mechanisms designed to ensure that concealment activities are only undertaken where reasonable, proportionate and necessary. For example, the AFP and the ACIC are required to notify the Inspector-General of Intelligence and Security (IGIS) that a thing was done to conceal access under a network activity warrant after the 28

[25] AFP Commissioner's Order on Operational Safety (CO3), Commissioner's Order on Operational Safety (CO3) (www.afp.gov.au)
[26] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 132.

day period following expiry of the warrant within 7 days after the thing was done (proposed section 49D of the Surveillance Devices Act).[27] As noted below in response to **Recommendation 20**, the Department will consider extending such a notification requirement for the AFP or the ACIC to notify the Ombudsman of post-warrant concealment activity carried out more than 28 days after a data disruption warrant has ceased to be in force, just as the requirement that exists currently in relation to computer access warrants.

Recommendation 14 – limitations on extensions of data disruption warrants

68. As with the other warrants in the Bill, data disruption warrants can be issued for an initial period of up to 90 days. The reasoning behind the ability for data disruption warrants to be issued for up to a period of 90 days (as with other surveillance warrants) is detailed in the Explanatory Memorandum[28] and in the Ministerial response to the Senate Standing Committee for the Scrutiny of Bills. The Department reiterates that this does not mean that all warrants will be issued for a period of 90 days. The period for which a warrant is in force will be determined by the issuing authority on a case-by-case basis.[29]

69. The Bill makes provision for an officer of the AFP or the ACIC to apply for an extension of the warrant to a Judge or an AAT member for a period not exceeding 90 days after the day the warrant would otherwise expire but for the extension. As noted in the Explanatory Memorandum, this is an important mechanism to build flexibility into the warrant process and account for extended investigations and unexpected circumstances.[30] The issuing authority must consider the same matters required to issue a warrant in the first instance, and be satisfied that the grounds on which the application for the warrant was made still exist. While warrants may be extended an unlimited amount of times, the applications for extensions will be subject to the same rigorous scrutiny as the initial application.

70. The AFP and the ACIC are required to report to the Minister for Home Affairs on the number of extensions and variations made to a warrant along with the reasons for why they were granted. The Ombudsman is empowered to inspect the AFP and the ACIC's records to determine the extent of their compliance with requirements for data disruption warrants. This will necessarily involve inspecting records made in relation to extensions and variations of warrants.

Recommendation 15 – no extraterritorial application of data disruption warrants

71. This Bill enables the AFP and the ACIC to take action against offenders—who are in Australia or who are Australian—committing serious Commonwealth crimes that harm our community. It is important that the AFP and the ACIC are able to target these offenders when, due to the globalised nature of communications and data storage, they have relevant data overseas. The AFP and the ACIC will only be permitted to exercise powers where the criminal activity is occurring online within Australia and offshore where the Australian community is being targeted or one or more Australians are involved in the offending.

72. This is in contrast to the role of the ASD which includes preventing and disrupting, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia (paragraph 7(1)(c) of the Intelligence Services Act). The role of the AFP and the ACIC is very different from the ASD's role in targeting people or organisations undertaking cybercrime outside Australia. The distinction between the AFP and the ACIC's functions, and that of the ASD, is demonstrated by the evidence given by Ms Rachel Noble PSM, Director-General of ASD, at the public hearing for this review:

> If [ASD] were working on that basis to disrupt and deter cybercrime and [they] form a reasonable assessment that an Australian or an Australian network might be involved, [it] stop[s] … [They] would stop work and be unable to hand that operational activity over to either

---

[27] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 132–133.
[28] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 33, para. 83.
[29] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 123.
[30] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 39

> the AFP or ACIC, which does actually in real life occur. In which circumstance, ASD officers are in a position of watching crime happen to Australian victims sometimes and not being able to hand it over anywhere.[31]

73. Australian offenders regularly interact with data held offshore, and conversely, the Australian community can be harmed using data hosted offshore. Transnational serious and organised crime groups operate with complete disregard for borders, and are increasingly choosing to conduct their activities in countries that are not favourable for Australian law enforcement activity. Removing the ability to access or disrupt data offshore with the permission from the relevant foreign country (as is proposed in relation to data disruption warrants and network activity warrants) will significantly constrain the AFP and the ACIC's ability to investigate serious criminality and access the information required to identify offenders or disrupt online criminal activity.

Recommendation 16 – no emergency authorisations for data disruption powers

74. As noted in the Ministerial response to the Senate Standing Committee for the Scrutiny of Bills, the ability to disrupt data, and the ability to take control of an account in emergency situations is important for ensuring that the AFP and the ACIC will be able to respond to rapidly evolving and serious threats in a timely and effective manner.[32] Emergency authorisations do not amount to warrants being internally issued. Within 48 hours of an emergency authorisation being given, approval must then be sought by application to a Judge or AAT member (for data disruption) or a magistrate (for account takeovers).

75. The modern criminal environment is fluid and fast-paced, and criminal plans can escalate rapidly in response to numerous external factors. The AFP advises that, due to criminals' use of anonymising technology and encryption, it could be that the AFP becomes aware of an escalation of criminal planning or intent with short notice—for example, in the counter-terrorism space, where there is significant risk to the community if offenders are not disrupted. In a situation where a code word is posted to alert criminal network members to commence criminal activities, an emergency authorisation for the disruption of data could be utilised to remove the code word, reduce its visibility to criminal network members, and disrupt the plot for criminal offending. Emergency authorisations will allow the AFP to more effectively react to changes that pose a significant risk to community safety.

76. In regard to the Law Council's recommendation that, instead of emergency authorisations, there be practical mechanisms to enable the making and determination of warrant applications in urgent cases, such mechanisms are already contained in the Bill. Under subsection 27KA(4) a law enforcement officer may make an unsworn application for a data disruption warrant if he or she believes that immediate disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences. Under section 27KB, applications for data disruption warrants can be made remotely by telephone, fax, email or any other means of communication, if it is impracticable for an application to be made in person. These provisions reinforce that emergency authorisations are not to be made where urgency and impracticability are the only barriers to applying for a warrant by the usual processes.

77. The Law Council made these same recommendations with respect to network activity warrants in Schedule 2 (see **Recommendation 36**). However, under the Bill as introduced, emergency authorisations are not available in relation to the activities authorised by network activity warrants. This is because the purpose of a network activity warrant is gathering intelligence, where it is not envisaged that law enforcement will need to respond to time-critical situations.[33]

---

[31] Ms Rachel Noble PSM (Director-General of ASD) *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 63
[32] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 130–131.
[33] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 131.

Recommendation 17 – 'last resort threshold' for emergency authorisations

78. Noting the serious and urgent circumstances in which emergency authorisations are designed to be used, a law enforcement officer must have a reasonable suspicion that there is an imminent risk of serious violence to a person or substantial damage to property and the disruption of data is immediately necessary for dealing with that risk. The circumstances must be so serious and the matter must be of such urgency that disruption of data is warranted, and that it is not practicable to apply for a data disruption warrant in the circumstances. Emergency authorisations are used only as a last resort. In the past five years, only one emergency authorisation under the Surveillance Devices Act has been issued.[34]

79. Decisions to give emergency authorisations are subject to external scrutiny after the fact. Before deciding to approve the giving of an emergency authorisation for the disruption of data, the eligible Judge or nominated AAT member must consider (amongst other things) the extent to which alternative methods could have been used to help reduce or avoid the risk, and how much the use of alternative methods would have prejudiced the safety of the person or property because of delay. In making these considerations, the issuing authority must be mindful of the intrusive nature of accessing and disrupting data held in the target computer. It is appropriate that these considerations are made by the Judge or AAT member, as the independent issuing authority, rather than the appropriate authorising officer as this provides independent scrutiny of decisions to apply for and give emergency authorisations.

80. The Department does not agree with the Law Council's recommendation that the authorising officer should be required to consider the likely impacts on third parties in deciding to approve the giving of an emergency authorisation. Emergency authorisations may only be given in extremely serious, urgent and often time-critical circumstances. Issuing authorities must subsequently consider whether to approve the giving of an emergency authorisation. The use of emergency authorisations will be overseen by the Ombudsman. These processes would identify any issues (individual or systemic) in relation to emergency authorisation impacts on third parties.

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

Disclosing the existence of an emergency authorisation where it is not approved

81. As noted in the Ministerial response to the Parliamentary Joint Committee on Human Rights, persons of interest or those who are subject to Commonwealth covert powers do not—and should not—have to be notified of the use of powers against them.[35] This is consistent practice for covert warrants under the Surveillance Devices Act and other Commonwealth legislation that confers covert powers upon law enforcement and security agencies, such as the TIA Act.

82. Regardless of whether or not the giving of an emergency authorisation was approved, requiring the AFP or the ACIC to disclose the existence of data disruption activity to the affected parties would be inherently harmful to law enforcement operations or capabilities, and / or Australia's national security. For example, knowing that a certain website or forum is being monitored by law enforcement may jeopardise months or years of law enforcement efforts to penetrate or dismantle criminal networks (such as online child sexual abuse groups). Even where the subject of a covert power has been cleared of any criminal activity or is notified after the conclusion of an investigation or operation, this does not necessarily reduce this risk. For example, the person who holds the account could inadvertently jeopardise future law enforcement investigations by publicly announcing they were subject to the warrant in relation to an account on a particular electronic service.

83. The Department acknowledges that the use of a covert power will affect a person's privacy, however these measures are balanced with strict safeguards, including restrictions on the use and disclosure of information obtained under an emergency authorisation (and any subsequent warrant), and robust

[34] An emergency authorisation for the use of a tracking device was granted to the AFP in 2018-2019, the Surveillance Devices Act 2004 Annual Report 2018–2019.
[35] *Ministerial Response to the Parliamentary Joint Committee on Human Rights – Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Report 3 (2021) p. 80.

oversight and reporting requirements. In particular, the Ombudsman and the IGIS will inspect and review agencies' use of the warrants in the Bill.

Requirement to take remedial action where an emergency authorisation is not approved

84. Where a person suffers loss of, or serious damage to, property or personal injury as a result of the execution of a warrant or an emergency authorisation, the Commonwealth is liable to compensate that person. This does not apply where a person has suffered the loss, damage or injury as a result of engaging in criminal activity. Compensation may be agreed to between the Commonwealth and the person or—in the absence of such an agreement—determined by action against the Commonwealth in a court of competent jurisdiction. See existing section 64 in the Surveillance Devices Act (in relation to data disruptions warrants and account takeover warrants) and proposed section 3ZZWA in the *Crimes Act 1914* (Crimes Act) (in relation to account takeover warrants).

85. Neither a data disruption warrant or emergency authorisation can authorise material interference with, interruption or obstruction of a communication in transit or a person's lawful use of a computer unless necessary to facilitate the execution of the warrant. A data disruption warrant or emergency authorisation also does not authorise causing any other material loss or damage to other persons lawfully using a computer, unless the loss or damage is justified and proportionate, having regard to the offences covered by the warrant.

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

86. Currently, the Bill provides that law enforcement officers of the AFP and the ACIC may apply to an 'appropriate authorising officer' to authorise the disruption of data or taking control of an account in certain emergency situations. In relation to the ACIC, 'appropriate authorising officer' is the CEO of the ACIC or an executive level member of the ACIC who is authorised by the CEO to be an appropriate authorising officer. This means that an executive level member of the ACIC is only able to give an emergency authorisation if they have been expressly authorised to do so by the CEO.

87. As noted in the Ministerial response to the Senate Standing Committee for the Scrutiny of Bills, the level of officer in the ACIC able to give an emergency authorisation differs to that in the AFP to reflect differences in the organisational structures and staffing arrangements.[36] There are circumstances where it is necessary and appropriate for the CEO of the ACIC to authorise executive level staff members to give emergency authorisations, where particular resourcing or operational needs require this. Importantly, such decisions will be made at the discretion of the CEO of the ACIC.[37]

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

88. The Department will give further consideration to the Law Council's recommendation that the AFP and ACIC should be required to notify the Ombudsman of concealment actions carried out in relation to data disruption warrants, consistent with the existing notification arrangements for computer access warrants.

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

89. In the 2020–21 Budget, the Government allocated $1.6 million for funding associated with Ombudsman oversight of the measures in the Assistance and Access Act and other cybercrime law enforcement powers until 30 June 2021. This funding was used to upgrade security infrastructure ($0.9 million) and to support oversight of the Assistance and Access Act ($0.6 million). Further funding to provide resources for oversight will be considered by Government through budget processes.

---

[36] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 154.
[37] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 154.

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

90. The Bill extends the Ombudsman's oversight role to the proposed data disruption warrants and account takeover warrants, while tasking the IGIS with oversight of network activity warrants. The inspection role of the Ombudsman reflects the Ombudsman's current statutory functions, including existing provisions for Ombudsman oversight of other warrants in the Surveillance Devices Act. The Bill does not seek to amend the Ombudsman's oversight functions more broadly. During the development of the Bill, the Department worked closely with the Office of the Commonwealth Ombudsman and the Office of the IGIS to ensure that the new warrants are supported by strong safeguards and review mechanisms, and that the oversight arrangements are consistent with the statutory functions of each of these bodies.

91. In its submission, the Ombudsman notes that while introducing IGIS oversight of the AFP and ACIC's use of electronic surveillance would mark a convergence of each of the bodies' stakeholder bases, this is consistent with the broader delineation of the bodies' respective roles. The Department notes that, in practice, there may not always be a clear delineation between the IGIS' oversight of the proposed network activity warrants, and the Ombudsman's oversight of data disruption warrants and account takeover warrants. To minimise the risk of duplication of oversight and ensure efficacy in respective oversight roles, the Bill contains provisions to facilitate information sharing between the Ombudsman and IGIS.

92. As noted in response to **Recommendation 39,** the Richardson Review recommended several changes to oversight by the Ombudsman under a new proposed electronic surveillance framework,[38] including that the Ombudsman have a broader mandate to assess agency compliance with electronic surveillance legislation. The Government agreed that the Ombudsman's oversight should be extended to assessing overall compliance with the new electronic surveillance legislation rather than being limited to record-keeping and destruction processes. The Department is considering the most effective way to make holistic change to electronic surveillance laws, including the expanded oversight role of the Ombudsman, as recommended by the Richardson Review. The powers introduced by this Bill (if passed) would be included in that reform.

93. The Department's responses below to **Recommendation 39** and **Recommendation 51** provide further justification as to the proposed oversight arrangements in the Bill.

Recommendation 23 – removal of Attorney-General's information certification power in subsection 9(3) of the Ombudsman Act, in relation to oversight of data disruption warrants

94. Subsection 9(3) of the *Ombudsman Act 1976* (Ombudsman Act) relates to the exercise of the Ombudsman's functions and powers under that Act, such as the conducting of own-motion investigations. To the extent that the Ombudsman is conducting inspections in accordance with the Surveillance Devices Act to assess compliance with the data disruption warrants regime, subsection 9(3) of the Ombudsman Act does not constrain the oversight abilities of the Ombudsman. Subsection 9(3) of the Ombudsman Act cannot be used to prevent the disclosure of information required under the Surveillance Devices Act in relation to the Ombudsman's inspection functions.

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

95. The Bill does not provide for any agency other than the AFP and the ACIC to execute data disruption warrants. The anticipated assistance that ASD may provide to the AFP and the ACIC in relation to data disruption will be facilitated through ASD's existing functions under paragraph 7(1)(e) of the Intelligence Services Act, and the information sharing provisions in the Surveillance Devices Act.[39] ASD's assistance under paragraph 7(1)(e) of the Intelligence Services Act will be overseen by the IGIS.

---

[38] Mr Dennis Richardson AC, *Comprehensive review of the legal framework governing the National Intelligence Community* (2019) Volume 2, p. 432–435.

[39] At existing subsection 45(4) (for data disruption warrants) and new subsection 45B(2) (for network activity warrants)

96. A formal request for ASD support under paragraph 7(1)(e) is initiated by a Government agency and considered by a senior ASD officer. Data accessed by ASD as part of a paragraph 7(1)(e) request is not used by ASD to perform the agency's own intelligence functions. However, a copy may be retained for audit purposes. ASD strictly complies with the *Rules to Protect the Privacy of Australians 2020*[40] (ASD Privacy Rules), issued by the Minister of Defence in accordance with section 15 of the Intelligence Services Act on 13 November 2020.

97. ASD's role is to provide technical support only to the AFP and ACIC under paragraph 7(1)(e) of the Intelligence Services Act. For example, ASD could provide advice and assistance on provision of training, techniques and tradecraft required for successful cyber operations, be involved in training on how to properly analyse and interpret the technical data that is obtained through these operations, or share or develop analytic tools.

98. Oversight arrangements for an ASD officer who is otherwise made available to the AFP or the ACIC would depend on the nature and terms upon which the ASD officer is made available. For example, a person could be employed by ASD and be seconded as a staff member of the AFP or the ACIC. Consistent with the ordinary meaning of a 'secondment', under such an arrangement the person would likely only have access to the powers and functions of an AFP or ACIC staff member, and not those available to an ASD staff member. In this scenario, the use of those powers and functions would be subject to oversight by the Ombudsman (except where it relates to a network activity warrant, which would be overseen by the IGIS). Conversely, if an ASD staff member is temporarily transferred to the AFP or the ACIC in a capacity that requires them to conduct activities for the purpose of ASD's functions under section 7 of the Intelligence Services Act, their activities would remain subject to IGIS oversight.

Recommendation 25 – additional Ministerial reporting requirements

Additional information to be included in the report on each warrant

99. The existing reporting requirements in relation to data disruption warrants as set out in the Bill already capture a number of the additional matters recommended by the Law Council. The AFP and the ACIC are required to report to the Minister for Home Affairs in relation to each warrant or emergency authorisation as soon as practicable after the warrant or authorisation ceases to be in force (proposed subsection 49(2D)). This is distinct from annual reporting requirements which require the AFP and the ACIC to provide relevant statistical information regarding the use of the warrants in respect of each financial year (existing section 50) (see below response to **Recommendation 26**).

100. The report to the Minister must include (amongst other things):

    a. the details of the access to, and disruption of, data under the warrant (proposed subsection 49(2D)). Depending on how data was accessed or disrupted under the warrant, this could include information relating to the exercise of telecommunications interception powers (if relevant), and

    b. the details of compliance with the conditions to which the warrant was subject (proposed subparagraph 49(2D)(d)(viii)). This will necessarily include information relating to the agency's compliance with statutory limits of authority, as recommended by the Law Council.

101. There are also reporting requirements for the AFP and the ACIC in relation to the extraterritorial operation of the warrants (proposed subsection 43C(7)). This ensures that, as soon as practicable after executing a data disruption warrant in a foreign country, where consent to that access or disruption is required, the AFP and the ACIC must give the Minister written evidence of agreement by an appropriate consenting official of the foreign country.

102. The Department will consider in further detail, in consultation with the AFP and the ACIC, whether it would be appropriate for the AFP and the ACIC to report on the likely extent to which the execution of the warrant resulted in the loss or damage to the data of persons lawfully using a computer, to the extent that this is able to be known.

---

[40] *Rules to Protect the Privacy of Australians 2020 | ASD Australian Signals Directorate*

Separate report on post-warrant concealment activity

103. The Department refers to its response in relation to **Recommendation 20** above. The Department will give further consideration to the Law Council's recommendation to expand the notification requirements to include post-warrant concealment activity to reflect those in relation to existing computer access warrants. The Department considers that the oversight of these activities sits most appropriately with the Ombudsman, consistent with the existing oversight role of the Ombudsman.

Recommendation 26 – additional annual reporting requirements

104. The Law Council's recommendation for additional reporting requirements to the Minister is inconsistent with the policy intent of the Ministerial reporting when combined with annual (public) reporting requirements for data disruption warrants. The annual reporting requirements are an important mechanism for ensuring transparency and accountability while also ensuring that operationally sensitive information is protected. High-level statistics on the use of data disruption warrants will be published in annual reports each financial year. It is appropriate that more detailed information on the use of warrants is included in reports to the Minister for Home Affairs.

105. In addition to these reporting requirements, the AFP and the ACIC must keep records about their use of these warrants, including in relation to decisions to grant, refuse or revoke warrants and how any information obtained has been communicated (existing sections 51, 52 and 53). This information will allow the Ombudsman to review data disruption warrants through inspections to determine compliance with law. The Ombudsman will report on the results of inspections to the Minister for Home Affairs bi-annually. These reports will include details on any instances of non-compliance with the requirements of the warrant. In accordance with existing subsection 61(2) of the Surveillance Devices Act, the Minister must table the Ombudsman reports in Parliament to provide assurance to the public in relation to the use of these powers.

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

Excluding information obtained under a data disruption warrant from being used in evidence

106. The Law Council's concerns include that there is a risk that officers executing data disruption warrants will tamper with evidence of an accused person's actions, that there are practical and legal difficulties in challenging evidence gathered under a data disruption warrant, and that there are further risks if ASD staff are engaged to perform acts of data disruption.

107. These issues were thoroughly explored in the development of the Bill. There are existing practices that address these issues. For example, the AFP has extensive experience with digital forensics and working with electronic evidence, to ensure information is appropriately secured and preserved. As a matter of forensic best practice, data will, where practicable, be copied and thereby preserved prior to any alteration. Where alteration of modification of data is required, these changes will be recorded, to account for such changes and identify how the data existed prior and post alteration. Furthermore, the rules of evidence will apply to evidence gathered under a data disruption warrant just as it applies to other warrants, meaning that, as the Law Council has stated, the court can exclude evidence if there is a suspicion that its integrity has been impaired.

Law Council alternative option – training etc for ASD staff members

108. The Law Council's alternative option appears to be based on a misapprehension of the nature and scope of any ASD involvement in the exercise of data disruption warrants by the AFP or ACIC. Any assistance ASD provides to the AFP or the ACIC would be in accordance with existing section 7(1)(e) of the Intelligence Services Act. Under that section, ASD may provide assistance to Commonwealth and State authorities in relation to cryptography, communication and computer technologies, and other specialised technologies acquired in connection with the performance of its other functions. As discussed in the response to the Law Council's **Recommendations 9** and **24** above, the type of assistance ASD can provide under section 7(1)(e) is limited, relevantly, to assistance in relation to specified technologies. This would not extend to any independent intelligence collection by ASD.

109. ASD has a deep understanding of the cyber threat environment and has developed technical expertise through the conduct of its own functions. ASD provides this expertise to other agencies, such as the AFP and the ACIC, to assist them to perform their own functions. ASD does not envisage any special training being required to perform the agency's existing function under section 7(1)(e) of the Intelligence Services Act.

Protection of data disruption technologies and methods

110. In addition, the Law Council recommends that proposed section 47B (pertaining to the protection of data disruption technologies and methods) be omitted from the Bill. However, capability protection is a fundamental tenet of covert investigations—proposed section 47B must be maintained to protect the techniques and capabilities deployed by the AFP and the ACIC in executing a data disruption warrant must be protected.

Independent review of the use of evidence

111. The Law Council also recommends that there should be an independent review of the use of evidence obtained under a data disruption warrant after an appropriate period of time. As outlined above, the Department is satisfied that any evidence collection risks associated with data disruption are appropriately controlled, also noting the Department's agreement to consider further limitations. This may limit the merit of an independent review into the operation of section 65C.

Recommendation 28 – permitted disclosures in relation to legal advice about a warrant issued under the Surveillance Devices Act

112. The policy intent of the use and disclosure provisions in the Surveillance Devices Act is not to prevent the use and disclosure of protected information for the purposes of obtaining legal advice relating to giving effect to provisions and purposes of the Surveillance Devices Act.

113. The Bill makes provision for protected information under the Surveillance Devices Act (including protected network activity warrant information) to be used, recorded, communicated or published in connection with the administration or execution of the Act (proposed paragraph 45B(4)(a) in Schedule 2 and item 2 of Schedule 5). These amendments would permit a person to use or disclose protected information for the purposes of obtaining legal advice that relates to giving effect to provisions or purposes of the Surveillance Devices Act. For example, for the purposes of obtaining legal advice about the execution of a warrant under the Surveillance Devices Act to which the person is connected.

114. To avoid any doubt, the Department will consider whether the ability to use or disclose protected information for the purposes of obtaining legal advice or initiating legal proceedings in connection with the powers in the Surveillance Devices Act could be further clarified through legislation or in explanatory materials.

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

115. Assistance orders are required to ensure that the AFP and ACIC can compel a specified person with relevant knowledge to provide information or assistance as is reasonable and necessary to carry out the warrant. The assistance order regime in the Bill is based on existing assistance orders available to law enforcement, in relation to computer access warrants under section 64A of the Surveillance Devices Act, and search warrants under section 3LA of the Crimes Act.

116. The computers targeted by the warrants in the Bill will often be protected by passwords and other layers of security. Assistance orders are designed to be used, for example, to compel a person to provide a password, PIN code, sequence or fingerprint necessary to unlock a computer or account that is the subject of a warrant. There may also be circumstances where it is necessary to compel a person to give assistance by disrupting data—for example, by requesting a system administrator remove an offender's access to a platform that they are using to conduct illegal activity.

117. The assistance requested under a data disruption assistance order must be reasonable and necessary to allow a law enforcement officer to either disrupt data that is the subject of a data disruption warrant or an emergency authorisation, access that data, copy that data, or convert that data into an intelligible

form. The Law Council has expressed a concern that an assistance order could be used to compel a person to inflict significant damage to their own commercial interests. However, assistance orders are only available in relation to a data disruption warrant (or emergency authorisation), and as such are subject to the same strict limitations on the causing of material loss or damage as the principal warrant or emergency authorisation. As outlined in the response to the Law Council's **Recommendation 9** above, the Bill contains strict protections to minimise any undue impact from the exercise of the new powers (including assistance orders) on members of the technology industry and the legitimate users of devices including strict limitations on interference and causing damage. In addition, the Commonwealth is liable to compensate a person who has suffered loss of or serious damage to property or personal injury as a result of the execution of the warrant, including when that execution involves an assistance order, (unless the loss, damage or injury was incurred as a result of engaging in criminal activity).

118. Assistance orders are not intended to compel assistance from a communications provider (for example, a telecommunications company), but rather from a specified person with relevant knowledge of a particular computer or a computer system or an online account. The AFP has confirmed that, from an operational perspective, the assistance order provisions introduced by this Bill do not replicate the industry assistance framework introduced by the Assistance and Access Act, and nor do they allow the AFP or the ACIC to circumvent the protections in this framework. The AFP has advised that it would not use the assistance order provisions to target individual employees of particular providers in circumstances where those persons would fall within the category of persons who could assist. In such circumstances, the AFP would use the industry assistance framework, where available, as the AFP currently does for any assistance needed from industry to execute computer access warrants.

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

119. The Department has addressed the Law Council's recommendation that only superior court judges may issue warrants and that public interest advocates should be appointed to act as contradictors above in response to the Law Council's **Recommendation 5** and **Recommendation 7**.

120. Applications for assistance orders should not be conducted on an *inter partes* basis. This is particularly the case because assistance orders may be served on suspects of criminal offences. An assistance order supporting a data disruption warrant may be given to a person who owns a computer that is used to access an encrypted messaging platform. It is likely that the person providing the assistance will also be a suspect, even if the assistance requested is for the purpose of frustrating the criminal offending of other participants to the serious crime (particularly if the data disruption warrant is used in conjunction with an account takeover warrant). The ACIC notes that an assistance order could be served on the administrator of a dedicated encrypted communications platform that is used explicitly by criminals to obscure their criminal activities.

121. It is highly likely that the specified exceptions identified by the Law Council—urgency, risks of prejudice to an operation, or safety and security—would be present during applications for these warrants, significantly limiting the utility of *inter partes* applications as the default position. Given the nature of the crimes being investigated under these warrants, there is also a significant risk that default *inter partes* applications would add an unacceptable and avoidable degree of risk that an operation would be prejudiced, particularly in time-critical circumstances, even where an order is served on a person who is not the suspect or an associate of the suspect.

122. The assistance order regime for each of the warrants in the Bill is modelled on existing provisions governing assistance orders, including computer access warrants (in section 64A of the Surveillance Devices Act). These assistance orders were introduced by the Assistance and Access Act which has been subject to a number of Parliamentary reviews and an INSLM review, none of which have made specific observations in relation to these orders.

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

123. In order to grant an assistance order in support of a data disruption warrant, an eligible Judge or nominated AAT member must be satisfied that disruption of data held in a computer is likely to substantially assist in frustrating the commission of relevant offences, and is justifiable and proportionate, having regard to the offences targeted. Further detail is set out in the Ministerial response to the Senate Standing Committee for the Scrutiny of Bills.[41]

124. Mandatory consideration of certain specified matters will inform the issuing authority's decisions to issue warrants and, in turn, inform decisions about whether to grant an assistance order. In recognition of the impact on privacy of third parties, the issuing authority is required to have regard to certain specified matters when deciding whether to issue the warrant (see the Ministerial responses to the Senate Standing Committee for the Scrutiny of Bills[42] and Parliamentary Joint Committee on Human Rights[43]).

125. The Department has addressed the Law Council's recommendation that the issuing authority be satisfied of necessity rather than justifiability in response to the Law Council's **Recommendation 4**, above.

Recommendation 32 – period of effect, content and form requirements for assistance orders

126. Assistance orders are not standalone orders, but rather can only be given in support of an underlying warrant while that warrant is in force. The warrants in the Bill can be in force for an initial period of up to 90 days, with the option to apply for an extension for an additional 90 days. The period for which assistance can be compelled under an assistance order cannot extend beyond the scope of the underlying warrant. Assistance orders can only be granted in respect of activity that is authorised by the underlying warrant. For example, a person can only be compelled to access or disrupt data held in a computer that is the subject of a data disruption warrant (or an emergency authorisation) for data disruption.

127. A key safeguard on the granting of assistance orders in relation to the three the warrants proposed in this Bill, is the requirement for the assistance to be reasonable and necessary to enable the law enforcement officer to carry out certain activities while executing the warrant. This would preclude the use of a single assistance order to compel a person to give assistance on an ongoing or repetitive basis where it is not reasonable and necessary to do so. It may be reasonable and necessary to compel ongoing or repeated assistance from a person who uses a particular computer, for example where the login credentials and passwords to that account are changed every month, but the operation runs over a period of three months and the agency requires repeated access.

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

128. The INSLM's recommendation to clarify that assistance orders do not authorise the detention of a person relates to the assistance order regimes in the Crimes Act and *Customs Act 1901* (Customs Act) (recommendation 17[44]), and in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act)(recommendation 23[45]). The INSLM did not make any specific recommendation in relation to the

---

[41] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 137-138.
[42] *Ministerial Response to the Senate Standing Scrutiny of Bills Committee - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 5 (2021) p. 136-137
[43] *Ministerial Response to the Parliamentary Joint Committee on Human Rights - Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Digest 3 (2021) p. 72-75
[44] Dr James Renwick CSC SC (Independent National Security Legislation Monitor), *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters'* (2020), Recommendation 17, p. 45
[45] Dr James Renwick CSC SC (Independent National Security Legislation Monitor), *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters'* (2020), Recommendation 23, p. 46

assistance orders in the Surveillance Devices Act (upon which the assistance orders in this Bill were modelled).

129. The Department responded to the INSLM's recommendation in its supplementary submission to the Committee's third review of the Assistance and Access Act. The Department confirmed that section 3LA of the Crimes Act and section 201A of the Customs Act (which require a person with relevant knowledge of a computer or computer system to assist with access under a search warrant) are not intended to authorise the detention of persons to whom the relevant orders apply, where the agency does not otherwise have any lawful basis to detain the person.[46] The assistance orders introduced by this Bill similarly do not authorise the detention of a person where the AFP or the ACIC does not otherwise have any lawful basis to detain the person.

Recommendation 34 – Ombudsman oversight of mandatory assistance orders

Notification for the execution of an assistance order

130. An assistance order supporting data disruption can only be used to compel a person to provide information or assistance to allow the law enforcement officer to access or disrupt data in a computer that is the subject of a data disruption warrant or emergency authorisation. Under proposed section 49C, the AFP and the ACIC are required to notify the Ombudsman of acts or things done under a data disruption warrant within 7 days of that thing being done. This would include notification when the AFP or the ACIC accessed or disrupted the data with the assistance of a person with relevant knowledge under an assistance order.

Power to enter premises and be present at the execution of an assistance order

131. It is not necessary to empower the Ombudsman to enter premises and be present during the execution of an assistance order. The Law Council makes this recommendation on the basis that assistance orders create a risk of arbitrary detention or other deprivation of liberty. As noted above in response to the Law Council's **Recommendation 33**, the assistance orders introduced by the Bill do not authorise the detention of a person where the agency in question does not otherwise have any lawful basis to detain the person.

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

132. The Bill does not contain a specific requirement for agencies to report on the use of assistance orders because those orders do not stand alone but rather, must be given in support of an underlying warrant. These underlying warrants are subject to their own Ministerial and annual reporting and record-keeping requirements. These are intended to capture circumstances where assistance given under an assistance order has supported the execution of the warrant.

Network activity warrants (Schedule 2)

Recommendation 36 – common issues with other warrant types

133. The Department refers to its corresponding responses above (**Recommendations 3, 5–7, 10–13, 15–19, 24** and **28–33**).

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

134. The current definition of a 'criminal network of individuals' set out in section 7A was drafted to ensure operational efficacy, and to account for the variety and complexity of technologies that agencies will encounter in seeking to prevent, detect and frustrate serious cyber-enabled crime. The definition is designed to capture individuals who did not intentionally facilitate criminal activity, or who may be

[46] Department of Home Affairs, *Supplementary submission to the [Parliamentary Joint Committee on Intelligence and Security] Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Submission 16.2) (2020) p. 10–11.

accessing the same electronic service as those who do have those intentions. It is necessary that these individuals fall within scope of the warrant because the devices they use may hold, or lead to, valuable intelligence about criminal activity. The breadth of this definition is balanced by the stringent criteria to obtain a network activity warrant and the limitations on the use of information obtained under the warrant for intelligence collection purposes only.

135. The criminal networks targeted by network activity warrants will not always be operating for a common criminal purpose—they may have multiple purposes and goals of which only some members are a part and carry out a range of serious crimes of differing gravity. For example, dark web marketplaces often have a wide range of users who are not operating for a common criminal purpose—some users may be trading in illicit substances or drugs, with other users only seeking stolen credit card or personal identification details.

136. Another example is dedicated encrypted communication platforms, such as Phantom Secure or Encrochat, which are commonly used by organised crime groups. Such organisations are frequently involved in multiple different types of offending.

137. Implementing the Law Council's recommendation could undermine the intended purpose of network activity warrants as an intelligence collection tool to identify unknown individuals and the scope of their offending. Only being able to target one criminal enterprise would be detrimental to law enforcement gaining a complete understanding of the group's criminal activities. It is the intelligence gathered under this warrant that may show the common criminal purpose as agencies may not have an accurate understanding of what criminal activity is being facilitated until they have access to devices used by the criminal network.

Recommendation 38 – power to authorise the use of surveillance devices

Power to use a surveillance device under a network activity warrant

138. The power to authorise the use of surveillance devices under network activity warrants does not constitute a trend towards a 'single electronic surveillance framework', as suggested by the Law Council. Rather, this limited and incidental use of surveillances devices reflects the challenges agencies face in combating serious cyber-enabled crime occurring in the increasingly complex modern communications environment.

139. It will often be necessary to use a surveillance device while executing a network activity warrant to make things authorised by the warrant possible, or to maintain the covert nature of the warrant. Similar to the case with permissible interception (see the response to **Recommendation 10,** above), the ability to use surveillance devices for the purposes of executing a network activity warrant enhances the operational effectiveness of that power, while also not detracting from the separate surveillance device warrants framework.

140. Surveillance device warrants and network activity warrants are for very different purposes: the collection of evidence by surveillance, in the case of a surveillance device warrant, and the collection of intelligence by access to data, in the case of network activity warrants. The threshold tests for application for a network activity warrant and surveillance device warrant are not (and should not be) aligned. The AFP and the ACIC will not use network activity warrant applications to circumvent the existing approval requirements for the use of surveillance devices to collect evidence.

141. Proposed subparagraphs 27KN(c)(i) and (ii) require that in circumstances where limited, incidental use of a surveillance device is authorised under a network activity warrant, the warrant must specify both the surveillance device which is authorised to be used, and the activities for which it may be used. Each of these matters will be considered by the issuing authority in determining whether or not to authorise limited, incidental use of a surveillance device in issuing a network activity warrant. A separate requirement to specifically approve surveillance activities is unnecessary.

Use and disclosure of information obtained from the use of a surveillance device

142. The Law Council raised concerns with the ability to use or disclose information obtained from the use of a surveillance device under a network activity warrant. However, this information can only be used,

recorded, communicated or published in accordance with proposed subsection 45B(7). Unlike other information obtained under a network activity warrant, information obtained from the use of a surveillance device cannot be used for intelligence purposes, or for making an application for another warrant. It is important that this information is dealt with differently to other information, as the purpose of this limited power to use surveillance devices is only to facilitate the execution of the warrant, not to collect intelligence through surveillance.

143. Information obtained from the use of a surveillance device may be used or disclosed for the purposes of an IGIS official exercising powers or performing its functions or duties (paragraph 47B(7)(b)). This ensures that the IGIS will be able to assess the legality and propriety of using a surveillance device under a network activity warrant. Paragraphs 45B(7)(c) and (d) ensure that this information can also be used or disclosed in an investigation or proceeding in relation to a contravention of the secrecy provisions. This ensures that where a person has unlawfully used or disclosed information obtained by using a surveillance device, he or she may be effectively investigated or prosecuted for the offence.

Recommendation 39 – oversight of network activity warrants

144. Any requests for funding to provide resources for oversight will be considered by Government through budget processes.

145. At the public hearing, the Ombudsman and IGIS explained their intention to work together to ensure that their respective roles build public confidence in the operation of the new powers.[47] This is supported by express provisions in the Bill facilitating information sharing between the Ombudsman and IGIS to address the bodies' concurrent jurisdiction and minimise risk of duplication of oversight.

146. The Department does not consider it appropriate to expand the Ombudsman's oversight role only in relation to the proposed powers in this Bill, but notes the Richardson Review's commentary in relation to this issue[48] (see the response to the Law Council's **Recommendation 22**, above).

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

147. The Department does not consider that the issuing process, thresholds or reporting requirements for ASIO's computer access warrants need to be reconsidered given the proposed network activity warrants, as these warrants do not create overlap between the respective intelligence collection functions for the AFP, the ACIC and ASIO. ASIO fulfils a different statutory function from the AFP and ACIC. ASIO's role is to collect intelligence to identify and investigate threats to security in line with its statutory functions under the ASIO Act. Unlike the AFP and the ACIC, ASIO is not charged with enforcing the criminal law.

148. The intelligence collected by the AFP or the ACIC under a network activity warrant must be linked to the prevention, detection or frustration of relevant offences, which is distinct from ASIO warrants that authorise the collection of intelligence on matters that are important in relation to security.[49] Even in the event that the relevant offence for a network activity warrant relates to subject matter covered by the definition of 'security' in the ASIO Act, the nature and objectives of the AFP and ACIC's criminal intelligence collection activities will differ materially from ASIO activities. ASIO, the AFP and the ACIC have longstanding cooperation and information sharing arrangements to coordinate their respective functions, avoid potential overlap and, where appropriate, facilitate joint operations.

---

[47] Mr Michael Manthorpe PSM (Commonwealth Ombudsman, Office of the Commonwealth Ombudsman) *Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Public hearing on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (10 March 2021) p. 39
[48] Mr Dennis Richardson AC, *Comprehensive review of the legal framework governing the National Intelligence Community* (2019) Volume 3, p. 129–131.
[49] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 334

149. The Richardson Review made recommendations to reform ASIO's computer access warrant framework, as part of the creation of a new electronic surveillance framework.[50] The Richardson Review also considered that the annual reporting requirements in a new electronic surveillance framework should be consistent with current arrangements.[51] The Government has agreed to these recommendations and any potential changes to ASIO's computer access warrants should be considered as part of these holistic reforms.

Account takeover warrants (Schedule 3)

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

150. In response to this recommendation, the Department refers to its corresponding responses above (**Recommendations 2, 3, 5**, **13**, **32** and **35**).

Recommendation 42 – justification for coercive account takeover powers

Justification for account takeover warrants

151. The Home Affairs principal submission explains the need for an account takeover warrant and the gap in the legislative framework that this warrant seeks to address.[52] The AFP's submissions to the Committee's review also provide further justification for the account takeover warrant from an operational perspective.

Ability to lock the account holder out of the account

152. To take control of an online account involves law enforcement taking steps that result in law enforcement's exclusive access to the account. In most cases, taking control of an online account will involve depriving the account holder or a user of their access to the account. This may facilitate the preservation of evidence, by ensuring that offenders cannot remove evidence of their criminality, but this is not the primary purpose. By enabling law enforcement to obtain exclusive control of an account, offenders are not able to alert other offenders of potential law enforcement activity, or otherwise knowingly or unwittingly compromise the integrity of the operation.

Recommendation 43 – definition of 'online account'

153. The current definition of 'online account' in section 3ZZUK is deliberately broad and technologically neutral. The type of accounts that may need to be taken over to enable evidence to be obtained vary immensely, contingent upon the unique circumstances of each investigation. Further explanation of the definition of 'online account,' the importance of capturing banking accounts, is outlined in the Home Affairs principal submission[53] and the Explanatory Memorandum[54].

154. It is important that the definition of an online account extend to sensitive accounts such as bank accounts and government services accounts. In some circumstances, access to a target bank account or government services account will be critical for revealing illicit financial flows, suspicious transactions or additional criminal actors, directly relevant to the crime being investigated. For example, live-stream child abuse material is increasingly being distributed in exchange for money or digital currencies, and access to banking or digital currency account activity will provide law enforcement with visibility of these illicit financial flows. The information gathered while in control of an account (under the authority of a

[50] Mr Dennis Richardson AC, *Comprehensive review of the legal framework governing the National Intelligence Community* (2019) Volume 3, recommendations 75, 76, 80–84, 86 and 103–105.
[51] Mr Dennis Richardson AC, *Comprehensive review of the legal framework governing the National Intelligence Community* (2019) Volume 3, p. 436–440.
[52] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p 10 and 16-17
[53] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p 19-20.
[54] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 40, 144 and 152

subsequent warrant or authorisation) will help identify other members of a criminal network, correlate patterns of illegal behaviour and provide a basis to apply for additional targeted warrants.

155. Government accounts and services, such as those with Centrelink, ATO, and Medicare, can form part of investigations into fraud, identity theft and the transfer of the proceeds of crime. It is important that the ACIC and the AFP are able to understand criminal behaviour and methodologies as well as to disrupt offending and prevent victimisation, for example to prevent the theft of superannuation. Further, in the course of investigating cyber or foreign interference offences targeting government offices and officials it is conceivable that systems definable as 'government accounts' may need to be subject to investigation. In a technology environment where online government accounts are likely to continue to be a key tool for individuals' interactions with government services, it is important to the future-proofing of this Bill and the protection of the community that those accounts be subject to these new warrants.

Recommendation 44 – requirement for affidavits

156. Account takeover warrants are a narrow power—they only authorise activities to enable the taking control of a person's online account. These warrants do not enable the direct collection of evidence (including access to data) while in control of the account. For these activities, the AFP and ACIC will need to use account takeover warrants in conjunction with other warrants (which may require affidavits) and/or authorisations.

157. Applications for account takeover warrants must provide sufficient information to enable a magistrate to decide whether or to issue the account takeover warrant (subsection 3ZZUN(3)). In addition, the magistrate may require the applicant to provide any additional information as he or she finds to be necessary to allow for the proper consideration of the application. There are other existing warrants in the Crimes Act which do not explicitly require the production of an affidavit—consistent with what is proposed for account takeover warrants—for example, search warrants.

Recommendation 45 – duration of warrants and authorisation of repetitive acts

Duration of account takeover warrants

158. It is not operationally feasible to require account takeover warrants to be executed within seven days of issuance, and for those warrants to cease to be in force once the AFP or ACIC has gained exclusive control of the account (akin to search warrants).

159. Search warrants authorise a discrete instance of evidence gathering in the investigation of a criminal offence through searches of persons or premises, and as such, can effectively cease to be in force once the evidence gathering exercise is complete. In contrast, an account takeover warrant is intended to be executed in tandem with more continuous methods of evidence collection and covert surveillance, as well as, controlled operations. Ongoing access to the online account is required to allow the flexibility needed to effectively infiltrate online criminality these subsequent investigatory powers. The AFP and the ACIC cannot remain in control of an account without an account takeover warrant, and as such the account takeover warrant must remain in force long enough to support evidence-gathering activities to be carried out (in conjunction with separate warrants or authorisations as required).

160. There may also be unscheduled occurrences, such as software updates or changes in technical code, which the AFP and the ACIC will need to take into account when executing the account takeover warrant. These occurrences may present challenges or opportunities for the effective execution of the warrant. Agencies are not able to predict the window within which these challenges or opportunities may present, and a seven day period of effect may be significantly limiting on the effectiveness of law enforcement action.

Where control of the account is lost

161. There is no requirement, and it is not operationally feasible for there to be a requirement, that the AFP or the ACIC maintain that control over the full period that the warrant is in place. For example, the AFP could lose control of an account due to a password reset. The AFP would need to regain control without delay, or risk revealing the existence of the operation to (or raising the suspicions of) suspects. Given the limited activity that an account takeover warrant enables, and the thresholds and safeguards

associated with the use of this warrant, the requirement to obtain a new warrant where control of the account is lost temporarily is unnecessary and disproportionate when considered against the operational risks.

Recommendation 46 – assessment of third-party impacts

162. In deciding whether to issue an account takeover warrant, the issuing authority must have regard to impacts on third parties by virtue of the mandatory conditions for issue in section 3ZZUP. Before issuing an account takeover warrant, the issuing authority must be satisfied that taking control of a person's online account is necessary for the purposes of enabling evidence to be obtained of the commission of relevant offences. In making this determination, the issuing authority must take into account certain specified matters at subsection 3ZZUP(2). These provisions support magistrates giving consideration to third party impacts that include, but are not limited to, privacy. The issuing criteria for account takeover warrants is explained in further detail in the Explanatory Memorandum[55] and the Home Affairs principal submission.[56]

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

163. Paragraph 3ZZUR(8)(a), as currently drafted, is an important safeguard against unjustified and disproportionate loss or damage to data. It will not be operationally feasible in the execution of an account takeover warrant to guarantee that there will be no loss of or damage to data in all circumstances. For example, in taking control of a person's account, it may be necessary to re-set or delete the settings on that account, which would involve loss of or damage to data. It is important to note that under subsection 3ZZUR(5), no material loss or damage to other persons lawfully using a computer is permitted under an account takeover warrant, even if this could otherwise be considered justified and proportionate.

Recommendation 48 – statutory compensation rights

164. Proposed section 3ZZWA, as currently drafted, provides that if a person suffers property loss, serious damage to property or personal injury in the course of, or as a direct result of, the execution of an account takeover warrant, the Commonwealth is liable to pay the person compensation. There are circumstances in which third party losses would be covered by this provision. Whether third party losses are covered would have to be considered on a case-by-case basis.

Recommendation 49 – notification requirement

165. The Department refers to the response to **Recommendation 18**, above, and the Ministerial response to the Parliamentary Joint Committee on Human Rights which outlines the risks associated with notification requirements for covert powers (regardless of whether the investigation against the person is ongoing or has concluded).[57]

166. The risks associated with a notification requirement remain, even though in practice some offenders would be aware that the AFP or the ACIC has taken control of their account, without a specific notification requirement. For example, the AFP or the ACIC may have previously asked for the offender's consent to take control of their account (which was then refused), or may have used an assistance order to compel the production of account credentials and passwords from the offender.

---

[55] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) p. 14-15 and 151-152
[56] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p 20-22
[57] *Ministerial Response to the Parliamentary Joint Committee on Human Rights – Scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Scrutiny Report 3 (2021) p. 80-81

Recommendation 50 – obligation to restore account access

Reasonable steps to restore account access

167. Proposed section 3ZZUV already provides that when an account takeover warrant ceases to be in force, the AFP and the ACIC must take all reasonable steps to restore an account holder's ability to operate their account if it will be lawful for the account-holder to operate it.

Changing the requirement to evaluate the lawfulness of holding an account

168. This provision ensures that the execution of an account takeover warrant is conducted in the same way, and with the same safeguards, where relevant and appropriate, as warrants that are conducted in the physical world, chiefly search warrants. The restoration of a person's account is intended to be equivalent to the return of a person's property once the investigation is no longer ongoing, and as long as holding that property is lawful.

169. In many circumstances, given the serious nature of the criminality being investigated under an account takeover warrant, evaluating the lawfulness of operating an account will not involve complex judgements by the AFP or the ACIC. For example, it is clear that the AFP and the ACIC should not be required to restore access to an account on the dark web used to run and administer a forum dedicated to child sexual abuse material. The Ombudsman will have oversight of the execution of this power, including the appropriateness of AFP and ACIC actions undertaken to return (or not return) the account.

Separate powers of investigation for further offending

170. The AFP advises that where there is a reasonable suspicion that an offence is occurring, the AFP will not use section 3ZZUV as a substitute for enforcement action as suggested by the Law Council. To do so would serve no practical purpose and would not be consistent with the criteria set out to obtain a warrant. Further, in some situations for overt takeovers, it may be that the AFP has already arrested the suspected offender who holds the account. In this situation, the purpose of the account takeover warrant is then to facilitate evidence collection and investigation into other unidentified offenders (e.g. through using a controlled operation and covert engagement).

Recommendation 51 – Ombudsman oversight of account takeover warrants

171. The Department has responded to the Law Council's recommendation in relation to reporting and record-keeping for mandatory assistance orders above in the response to **Recommendation 35**, and the Law Council's recommendation in relation to expanding the Ombudsman's oversight role in response to **Recommendations 22** and **39**.

172. In relation to the Law Council's recommendation to notify the Ombudsman of loss or damage, the Department considers that an additional notification requirement to the Ombudsman is unnecessary (see responses above to **Recommendation 20** and **Recommendation 9**). Proposed subsection 3ZZUR(5) provides that an account takeover warrant does not authorise materially interfering with, interrupting or obstructing a communication in transit or the lawful use of a computer. Neither do these warrants authorise causing material loss or damage to persons lawfully using a computer, that is, a third party. Proposed paragraph 3ZZUR(8)(a) ensures that the necessary interaction with data involved in the execution of an account takeover warrant has to be justified and proportionate.

Recommendation 52 – specific protections: legally privileged and confidential journalistic information

173. The data disruption warrants, network activity warrants and account takeover warrants proposed in this Bill apply equally to all individuals, including lawyers and journalists, noting that the powers can only be used where rigorous legislative thresholds are met. These powers do not override the principle of client-legal privilege. Communications to which privilege attaches cannot lawfully be seized under warrant.

174. The AFP and the ACIC advise that they have established protocols in place to manage client-legal privilege in the context of their existing covert investigatory powers. For example, the AFP and the Law Council have established *General guidelines between the Australian Federal Police and the Law Council*

of Australia as to the execution of search warrants on lawyers' premises, law societies and like institutions in circumstances where a claim of legal professional privilege is made. While these guidelines are focused on search warrants issued pursuant to the Crimes Act, the guidelines are interpreted as applying to warrants issued under other Commonwealth legislation on lawyers' premises or Law Societies where a claim of legal professional privilege is made. The Department has addressed the Law Council's recommendation that only superior court judges should issue warrants and that public interest advocates should be appointed to act as contradictors above in response to **Recommendations 5** and **7**.

Recommendation 53 – safeguards against exposure to multiple assistance orders

175. The Department refers to its response to **Recommendation 32**, above (in relation to assistance orders introduced by this Bill. The same principles apply to existing assistance orders).

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

Forthcoming corrections to the Explanatory Memorandum

176. As pointed out by the Law Council and the Department in our principal submission, the statement of compatibility with human rights in the Explanatory Memorandum currently, and incorrectly, states that the Bill excludes judicial review under the ADJR Act. The Department's forthcoming corrections to the Explanatory Memorandum will further explain the effect of section 9A of the ADJR Act in relation to data disruption warrants, network activity warrants and account takeover warrants.

ADJR application to other intelligence warrants

177. It continues to be appropriate that ASIO warrants be excluded from judicial review under the ADJR Act. ASIO fulfils a different statutory function from the AFP and ACIC. (as discussed in the response to **Recommendation 40**, above).

178. The 2012 Administrative Review Council's *Federal Judicial Review in Australia* concluded that national security considerations may be a reason for excluding ADJR review, in particular where sensitive information is involved which increased litigation in the area may potentially expose.[58] Decisions relating to the issue of ASIO's computer access warrants involve highly sensitive information relating to the conduct of ASIO's ongoing investigations, technical capabilities and methods, and intelligence that forms part of the facts and grounds supporting the warrant applications. It would not be appropriate that a decision to issue ASIO warrants be subject to judicial review under the ADJR Act, as review could adversely affect the effectiveness and outcomes of a security investigation. This is consistent with similar exclusions made for national security purposes, including decisions made under the Intelligence Services Act and the TIA Act, as listed in Schedule 1 of the ADJR.

179. While network activity warrants will be used by the AFP and the ACIC to build an intelligence picture, network activity warrants are intended to inform these agencies' use of more targeted evidence collection powers. As such, the Bill enables network activity warrants to be challenged. To make information available in order to bring about such a challenge, the Bill ensures that information obtained under a network activity warrant may be admitted into evidence in proceedings that are not criminal proceedings.

180. Regardless of the exclusions listed in Schedule 1 of the ADJR Act, Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia under s 75(v) of the Australian Constitution and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*.

[58] Administrative Review Council (ARC), *Federal Judicial Review in Australia*, ARC Report 50 (2012) p. 107, para. 5.118.

Recommendation 55 – sunset clauses and statutory review functions

Sunset clause

181. The Department does not accept the Law Council's contention that the nature of the new warrant-based powers is justification for the Bill being subject to a sunset clause. While the new powers are intrusive and designed to be used covertly, they are not inherently more extraordinary than the existing intrusive and covert powers available to the AFP and ACIC in the TIA Act and Surveillance Devices Act. As with all existing powers in the TIA Act and the Surveillance Devices Act, the new powers are subject to an extensive range of safeguards and robust oversight arrangements. What sets the new powers apart is that they are designed to address the new advancements in technology that threaten our law enforcement agencies' ability to keep Australians safe.

Expanding the remit and resourcing of the INSLM to cover the operation of the new warrant-based powers

182. The Department would engage closely with any review by the INSLM and/or the Committee of the powers introduced by this Bill.

183. Any resourcing needs of the INSLM and the Committee would be considered through Government processes.

184. Neither the Committee nor the INSLM should be specifically empowered to oversee the new warrants proposed by this Bill in an operational sense. This oversight role will sit with the Ombudsman and the IGIS.

Independent and Parliamentary oversight arrangements for national security legislation

185. The Department appreciates the importance and value of INSLM and Parliamentary oversight of criminal investigation powers and offences, including where those have national security implications. The Department will work with relevant agencies to consider these arrangements. The development of any legislative amendments (if ultimately considered to be required), and any resourcing needs of the Committee and the INSLM, would be considered through Government processes.

Australian Government Legislation Handbook

186. The Legislation Handbook is a whole-of-government document, which provides advice to all departments on the development of legislation, and the processes associated with legislation going through Parliamentary review and consideration. National security legislation is unique and relevant to only a few government departments. Further, the matters raised in the Law Council's recommendation are policy issues that should be considered by the Government on a case-by-case basis in relation to each proposed piece of legislation. The Department of the Prime Minister and Cabinet, which is responsible for the Legislation Handbook, does not support the Law Council's recommendation.

187. In accordance with existing Chapter 5 of the Legislation Handbook, in developing new legislation and amending existing legislation, the Department of Home Affairs will continue to consider whether a mechanism for reviewing legislation should be included. The Legislation Handbook provides that such a provision could require a one-off or regular review and specify those matters to be considered. For example, a provision could require regular consideration of whether the legislation: (a) is operating in a way that is legally effective to implement government policy, (b) has resulted in any unintended legislative consequences, (c) remains relevant and clear, or (d) contains any outdated or redundant provisions.[59]

Recommendation 56 – omission of Schedule 4 to the Bill

188. The amendments proposed in Schedule 4 are important for the effective operation of controlled operations online in the modern communications environment. The purpose of the amendments in

[59] Department of the Prime Minister and Cabinet, *Australian Government Legislation Handbook*, Chapter 5: Preparation of Drafting Instructions, p 26

Schedule 4 is to enhance the ability of the AFP and the ACIC to conduct controlled operations online (see the Home Affairs principal submission[60] and Explanatory Memorandum[61]).

189. The Law Council's interpretation of these provisions does not fully take into account the complexities of online operations. The nature of the material which is likely to be subject of a controlled operation conducted online (such as images, videos, livestream, chat pages) necessarily means that it can be much more easily forwarded, copied or transferred than is possible with physical goods. The existing wording in paragraph 15GI(2)(d) of the Crimes Act referring to illicit goods 'being under control of an Australian law enforcement officer at the end of the controlled operation' appears to contemplate physical goods rather than illegal online content.

190. As an example, the AFP may conduct a controlled operation to gather evidence as part of an investigation into the sale of stolen Australian identity documents on a dark web forum. The AFP might purchase those illicit goods (the stolen IDs) as part of the controlled operation, but law enforcement cannot guarantee that they have purchased the only copy or that they will have all copies in their possession at the end of the operation. The requirement to satisfy the 'to the maximum extent possible' threshold places an obligation on law enforcement to ensure that as many copies of the stolen IDs are under their possession, where this will not always be the most practical and effective use of investigative resources in conducting a controlled operation online.

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

191. Existing section 15HC of the Crimes Act ensures that the controlled operations framework in Part IAB cannot be used as a substitute for other laws.[62] Existing subsection 15HC(f) of the Crimes Act provides that a controlled operation cannot authorise, or confer criminal immunity or civil indemnity for, activities that could have been authorised under law relating to electronic surveillance devices or telecommunications interception. It is intended that this provision (or subsection 15HC(i) in relation to laws relating to any other matter concerning powers of criminal investigation) would capture data disruption warrants and network activity warrants.

192. Section 15HC is intentionally drafted in a way that is not overly proscriptive and does not describe the effects of every excluded warrant type in detail. This allows the provision to adapt to new modernised powers as they are introduced. However, the Department will consider whether an amendment or a legislative note could clarify, for avoidance of doubt, that a controlled operation cannot authorise, or confer criminal immunity or civil indemnity for, activities authorised by a data disruption warrant or a network activity warrant.

Response to the Law Council of Australia supplementary submission

193. At the public hearing for this review, the Law Council undertook to provide responses to two questions on notice regarding its recommendation to limit issuing authorities for the three new warrant types to superior court judges and international comparators with the proposed powers in the Bill. On 31 March 2021, the Law Council made a supplementary submission to the Committee responding to those questions on notice.

Question 1 – issuing authorities for existing electronic surveillance warrants

194. The Law Council provided reference to publicly available information concerning data held by the AAT about the length of time spent by relevant AAT members in determining warrant applications. For the reasons outlined above in response to Law Council **Recommendation 5**, the Department considers it

[60] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p 17
[61] *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020: Explanatory Memorandum* (2020) pp 180–181
[62] *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009: Explanatory Memorandum* (2009) p 75

appropriate that the proposed data disruption warrants and network activity warrants be issued by nominated AAT members, in addition to eligible Judges. The length of time necessary to determine a warrant application is referrable to the circumstances of each warrant application, and would not necessarily change if the issuing authority was a superior court judge rather than a relevant AAT member.

Question 2 – international comparators with the proposed powers in the Bill

195. The Law Council provided information about international comparisons with the proposed powers in the Bill from among Five Eyes partners, concerning the existence and scope of the powers, and authorisation requirements.

196. The Department notes that, as the Law Council has pointed out, the Five Eyes jurisdictions do not offer legislative frameworks or individual powers that are exactly equivalent to the powers in the Bill. The Department also notes and agrees with the Cyber Security Cooperative Research Centre's (CSCRC) supplementary submission to the Committee's review. The CSCRC noted:

> Given the diversity of legislative mechanisms, law enforcement and intelligence functions across the Five Eyes, it is difficult to make direct comparisons with the measures proposed in the SLAID Bill. However, it is important to note that our allies also recognise the threats posed by the dark web and anonymising technologies and the distinct and unique challenges they present for law enforcement. Hence, steps have been taken by several Five Eyes' states – namely the United States, the United Kingdom and Canada – to counter the proliferation of crime committed on the dark web and via anonymising technologies.[63]

197. The roles of agencies, and the legislative frameworks that underpin their powers, are all tailored to each jurisdiction's particular circumstances and legal requirements. In considering international models, the differences in agencies' roles and functions and the legislative frameworks underpinning their activities must be considered. In most cases, a direct comparison cannot be made. Directly equivalent legislative frameworks would not necessarily be appropriate or effective.

198. The powers proposed in this Bill have been carefully crafted in the Australian context to be effective, in both an operational and technical sense, and proportionate—in terms of authorisation frameworks, safeguards and oversight. The Bill provides the AFP and the ACIC with measured and targeted powers to respond to increasing criminal take up of sophisticated technologies to perpetuate serious offending.

Existing powers under the controlled operations regime in Part IAB of the Crimes Act

199. The Law Council contends that no particulars have been provided about the perceived limitations in existing powers under the controlled operations regime in Part IAB of the Crimes Act to undertake data disruption activities, in reliance on the statutory immunities for acts specified in an authorisation to conduct a controlled operation.

200. However, traditional law enforcement powers available to the AFP are framed by reference to action that is primarily focused on the gathering of evidence for use in a criminal investigation or prosecution. Enforcing the criminal law goes beyond just collecting evidence.

201. The controlled operations framework enables the collection of evidence that may lead to the prosecution of a person for a serious offence, and allows for the authorisation of conduct that would otherwise be unlawful, under specific constraints. During the development of the Bill, consideration was given to how far the controlled operations framework would extend in authorising disruption activity and account takeover activity. While controlled operations are able to authorise controlled conduct that is not otherwise provided for under law, they generally cannot be used to fill a gap in the suite of computer access powers available to the AFP and the ACIC in Commonwealth legislation. This is especially so given that controlled operations authorities are internally issued, whereas analogous investigative

[63] Cyber Security Cooperative Research Centre supplementary submission *[Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 14.1)

powers generally require a warrant to be issued externally to the agency.[64] The policy intent behind the Bill was to create a warrant-based framework where appropriate.

Ability to use existing investigatory warrants – particularly computer access warrants

202. The Law Council contends that there are existing investigatory warrants that could be used to combat technological difficulties in identifying and locating suspects at the early stages of an investigation, negating the necessity for the new powers in the Bill. The Law Council points in particular to subparagraph 27A(1)(c)(ii) and section 27F of the Surveillance Devices Act. These provisions relate to computer access warrants.

203. Computer access warrants are an evidence-gathering tool, and applicants of computer access warrants have to meet the thresholds set out in section 27A. However, the challenges associated with the dark web and anonymising technologies make meeting this threshold in certain contexts increasingly difficult. As noted in the Home Affairs principal submission, one such limitation is when law enforcement is seeking to map out the criminal landscape before targeting their evidence-gathering inquiries, that is, in the discovery phase of an investigation before the threshold to apply for a computer access warrant can be met. This is one of the key reasons for the development of network activity warrants. Similarly, data disruption warrants are available for a very different purpose, and in a different phase of an investigation, than computer access warrants. Data disruption warrants are for the purpose of frustrating criminal offences, and computer access warrants are for gathering evidence. The Home Affairs principal submission contains more information on the threat environment and the need for reform.[65]

Responses to questions on notice

204. The below provides the Department's response to questions taken on notice at the public hearing, as well as a response to a written question on notice from the Committee. A full list of questions on notice is provided at **Attachment B**.

Non-legally qualified Administrative Appeals Tribunal (AAT) members

205. At the public hearing, the Hon Mark Dreyfus QC MP asked the Department:

> ***Going to the justification about AAT members being legal practitioners, the AAT has told Senate estimates that there's a nominated AAT member for the purpose of the Surveillance Devices Act who was not enrolled as a legal practitioner of the High Court or of another Federal Court or Supreme Court of the state. Do you think it's appropriate for an individual with no legal qualifications to issue any of these three warrants that are in this bill?***

Nominated AAT members under the Surveillance Devices Act

206. Warrants in the Surveillance Devices Act, including the proposed data disruption warrants and network activity warrants, are issued by eligible Judges or nominated AAT members. For the reasons set out above in response to Law Council **Recommendation 5**, the Department considers it appropriate that data disruption warrants and network activity warrants be issued by nominated AAT members, in addition to eligible Judges.

207. The procedure for declaring eligible Judges and nominating AAT members for the purposes of issuing warrants is set out in sections 12 and 13 of the Surveillance Devices Act. Existing section 13 provides that the Attorney-General may nominate a person who holds a Deputy President, senior member or member appointment to the AAT to issue warrants under that Act. A Deputy President or a full-time senior member is not required to be enrolled as a legal practitioner to be nominated under section 13. A part-time senior member or a part-time or full-time member of the AAT may only be nominated if the

[64] Department of Home Affairs principal submission to the Parliamentary Joint Committee on Intelligence and Security review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, p. 9

[65] *Home Affairs Portfolio submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Surveillance Legislation Amendment* (*Identify and Disrupt) Bill 2020*, (Submission 9), p. 8.

person has been enrolled as a legal practitioner of the High Court, another federal court, or of the Supreme Court of a State or the Australian Capital Territory for at least five years. This is the same procedure for nominated AAT members for the purposes of issuing interception warrants in the TIA Act.

208. Under section 7 of the *Administrative Appeals Tribunal Act 1975*, a person may be appointed as a Deputy President, senior member or member of the AAT if they have been enrolled as a legal practitioner of the High Court or the Supreme Court of a State or Territory for at least 5 years or if, in the opinion of the Governor-General, they have special knowledge or skills relevant to the duties of a Deputy President, senior member or member. There is currently one AAT member who is nominated for the purposes of issuing warrants in the Surveillance Devices Act who does not have legal qualifications.

Amendments made by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

209. In responding to Mr Dreyfus' question at the hearing, the Department noted that the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill) (currently before Parliament) contains a legislative fix to resolve an error in relation to nominated AAT members under the TIA Act. By way of clarification, this is a separate matter. The IPO Bill makes minor amendments to section 6DA of the TIA Act to remove a redundant reference to 'Part 3-3' (stored communications) warrants being included in the nominations for AAT members able to issue interception warrants. Only 'issuing authorities' (including AAT members) appointed under section 6DB are able issue stored communications warrants. In substance, the IPO Bill does not change which Judges or nominated AAT members can authorise warrants under the TIA Act or the Surveillance Devices Act.

Definition of 'relevant offence' – offences against fisheries Acts

210. At the public hearing, the Committee Chair, Senator James Paterson, asked the Department whether the definition of 'relevant offence' in section 6 of the Surveillance Devices Act would apply to the Bill, and whether offences against the *Fisheries Management Act 1991* and the *Torres Straight Fisheries Act 1984* would hence also apply.

Fisheries Act offences in the Surveillance Devices Act

211. The offences in the *Fisheries Management Act 1991* (Fisheries Management Act) and *Torres Strait Fisheries Act 1984* (Torres Strait Fisheries Act) have been included in the definition of 'relevant offence' in section 6 of the Surveillance Devices Act since commencement in 2004, and when the Act was amended in 2007 by the *Fisheries Legislation Amendment Act 2007*. As noted in the Explanatory Memorandum to the Surveillance Devices Bill 2004, surveillance devices may be used for certain offences against the Fisheries Management Act to help Australia combat the serious problem of illegal fishing in the Australian Fishing Zone, such as the illegal fishing of Patagonian tooth fish. This ensures that surveillance devices may be used to assist with the investigation and prosecution of serious illegal fishing offences.

212. These foreign vessels fisheries offences are generally punishable on conviction with significant fines of at least 2,500 penalty units (approximately $555,000), up to 7,500 penalty units (approximately $1,665,000). These fisheries offences do not attract a penalty of a minimum term of imprisonment, in part because the United Nations Convention on the Law of the Sea prevents the imprisonment of persons on foreign vessels caught fishing illegally in a country's fishing zone.

213. The Australian Fisheries Management Authority (AFMA) is the authority responsible for investigating offences under these fisheries Acts. AFMA is not a 'law enforcement agency' and therefore its officers are not able to directly seek warrants under the Surveillance Devices Act in respect of these offences. However, AFMA may seek to work with a law enforcement agency to obtain and execute warrants in the Surveillance Devices Act in respect of these offences where the activities are also within the other agency's functions to investigate.

Interaction with the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

214. The proposed data disruption warrants and network activity warrants may be sought in respect of relevant offences in the Surveillance Devices Act, including the fisheries offences discussed above.

215. Any use of powers in the Bill for investigating these offences would be dependent on the particular investigation, and whether the powers were useful in that context. The AFP takes a lead role investigating environmental crime where the complexity, sensitivity or degree of harm caused to the environment necessitates the AFP's involvement as the lead investigating authority. However, the AFP generally implements a joint agency approach to investigation into environmental crime, enabling the specialist capabilities and resources of other agencies to be used.

Recommendation made by the Communications Alliance in relation to assistance orders

216. Following the public hearing for this review on 10 March 2021, the Committee Chair, Senator James Paterson asked:

> ***What would be the effect of following the Communications Alliance's recommendations that Assistance Orders should be directed to business users not intermediaries and to corporate entities not individual employees?***[66]

217. The recommendation from the Communications Alliance that assistance orders should be directed to business users not intermediaries, and to corporate entities not individual employees, is based on a misunderstanding of the purpose and policy intent of assistance orders. Assistance orders are not intended to compel assistance from a communications provider (or corporate entities) or from the employees of those providers, but rather from a person with relevant knowledge of a particular computer, computer system or online account. For example, an order could be sought to require an individual who uses a particular computer, or shares access to a particular account, to provide the password.

218. Should the AFP and ACIC wish to seek assistance from the communications industry to facilitate the execution of these warrants, this would occur through existing mechanisms such as the industry assistance framework in Part 15 of the *Telecommunications Act 1997* (Telecommunications Act), introduced by the Assistance and Access Act. The industry assistance framework provides an established structure for seeking assistance from communications providers, including consultation requirements and immunities relating to the provision of assistance. Requests or notices must be served on the entity that is the designated communications provider, not on individual employees.

219. The assistance order regime in the Bill is based on existing assistance orders available to law enforcement, in relation to computer access warrants under section 64A of the Surveillance Devices Act, and search warrants under section 3LA of the Crimes Act. Assistance orders for computer access warrants were introduced by Schedule 2 of the Assistance and Access Act as a mechanism to seek assistance from specific individuals with relevant knowledge of a particular computer, being a circumstance not covered by the industry assistance framework introduced by Schedule 1 of the same Act. As noted by the third INSLM in his review of the Assistance and Access Act:

> Assistance orders are distinct from — and ought not be confused with — industry assistance orders in Part 15 of the Telecommunications Act, as amended by Schedule 1 of [the Assistance and Access Act]. Though there are many distinctions between assistance orders and industry assistance orders, chief among them is the fact that assistance orders [are] issued in respect of an individual or natural person, not a [designated communications provider].[67]

[66] Mr John Stanton, *Communications Alliance submission to the Parliamentary Joint Committee on Intelligence and Security review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (Submission 12), p. 4, para 7.
[67] Dr James Renwick CSC SC (Independent National Security Legislation Monitor), *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters'* (2020) p. 243, para 12.72.

Attachment A – Law Council 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 necessary 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 all types 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 ex 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 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.

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

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).

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).

Attachment B – List of questions on notice

Questions taken on notice at the public hearing

Non-legally qualified AAT members

Mr DREYFUS: *Going to the justification about AAT members being legal practitioners, the AAT has told Senate estimates that there's a nominated AAT member for the purpose of the Surveillance Devices Act who was not enrolled as a legal practitioner of the High Court or of another Federal Court or Supreme Court of the state. Do you think it's appropriate for an individual with no legal qualifications to issue any of these three warrants that are in this bill?*

Mr Kershaw: *That's really a matter for the AAT.*

Mr DREYFUS: *No, it's not. The Surveillance Devices Act uses the phrase 'nominated AAT member'.*

Mr Warnes: *We're aware of that issue and aware of that error on the face of the Surveillance Devices Act. I'm happy to correct this on the record if I get it wrong, but my recollection is that the IPO bill that's currently before the parliament has a fix for that, to correct that error. We are aware of that and looking to correct it through legislation that's in parliament and is being heard by this committee.*

Mr DREYFUS: *I'll be very pleased if that's the case, but do you think that that's a matter that should have been drawn to the committee's attention in the Home Affairs portfolio submission, if it is, in fact, the case?*

Mr Warnes: *I'm sorry, but I can't recall if it was set out in the explanatory memorandum for the IPO legislation or in the submission. I just can't recall.*

Mr DREYFUS: *Could you confirm that in writing for the committee, because it's an important matter. It goes to who is to issue what, as I've said, many people have described as 'extraordinary warrants'.*

Mr Warnes: *Yes, I'm absolutely happy to take that on notice and provide you with some more information on the IPO bill and the fix that's there.*

Definition of 'relevant offence' – offences against fisheries Acts

CHAIR (Senator Paterson): *I'm reading here from the definition section, section 6, of the SD Act, so perhaps this relates to previous powers, not the new powers. It lists a range of things, including the three-year threshold, and amongst it is the Fisheries Management Act 1991 or the Torres Strait Fisheries Act 1984.*

Mr Warnes: *Apologies, I thought you were referring to our legislation, the amending bill. I don't have an answer as to why that was there. I assume in the previous regime it was thought appropriate to put them in there for surveillance devices.*

CHAIR (Senator Paterson): *But am I right in understanding that, if this act were amended according to the draft bill, it would pick up those definitions?*

Mr Warnes: *It picks up the definitions in the current act. That's correct.*

CHAIR (Senator Paterson): *I would be very interested to know how it could potentially be used in the enforcement of those two acts.*

Mr Warnes: *As I was saying, I'm not sure that it could be used in the enforcement of those acts, because the AFP don't investigate those offences and only the AFP can use those powers. I'm happy to take that on notice and see if there's any correction to that.*

Written questions on notice

Responses to recommendations made by the Law Council of Australia

The Committee as a whole ask that the Department provide a response to each of the Law Council's recommendations. It would greatly assist if, in doing so, the Department consider both legal and operational

impacts. Please note that some members may not feel that 'to maintain consistency with existing powers in the Acts' is a sufficient response.

Response to recommendation made by the Communications Alliance

The Committee Chair (Senator James Patterson) asked: What would be the effect of following the Communications Alliance's recommendations that Assistance Orders should be directed to business users not intermediaries and to corporate entities not individual employees?

The relevant part of the submission (Submission 12, p. 4) states as follows:

> *Assistance Orders*
>
> *The proposed new Sections 64A and 64B of the amended SD Act would allow law enforcement agencies to compel specified persons to provide reasonable information and assistance to agencies aimed at the execution of a warrant. Therefore, it is possible that communications platform providers could be captured in the potential net of recipients of such assistance orders. However, such orders would be more appropriately directed at either the (business) user (first priority) of such platforms that holds or manages the account in relation to which access is sought or the platform provider corporation rather an individual employee or officer. If, as a last resort, an assistance order is directed at an individual employee or officer (rather than the business user or the platform corporation), this may give rise to a conflict between the order and the employee's work responsibilities/terms of employment. It may also create difficult situations regarding the extent to which communications and approval within the employer organisation is prevented because of the legal constrains pertaining to protected information. The Bill should address these issues by requiring that the technology provider organisation be the target of technical assistance requests and, where an individual is compelled to provide assistance, by facilitating and paying for independent legal advice and to protect the employee from possible adverse consequences (both in terms of damages and employment) arising from compliance with the order.*