31 March 2021

Law Council
OF AUSTRALIA

Office of the President

Senator James Paterson
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

By email: pjcis@aph.gov.au

Dear Chair

SURVEILLANCE LEGISLATION AMENDMENT (IDENTIFY AND DISRUPT) BILL 2020

1. Thank you for the opportunity to appear at the Committee's public hearing on 10 March 2021, as part of its review of the above Bill. This correspondence addresses two matters that Law Council witnesses took on notice at the hearing, namely:

   - Senator the Hon Kristina Keneally asked the Law Council about its recommendation to limit issuing authorities for the three new warrant types to superior court judges, and the basis for its concerns about the appointment of members of the Administrative Appeals Tribunal (**AAT**) as issuing authorities. The Law Council undertook to provide a reference to relevant publicly available information concerning data held by the AAT about the length of time spent by relevant AAT members in determining warrant applications; and
   - during questioning by the Hon Mark Dreyfus QC MP, the Law Council offered to provide further information about international comparators with the proposed powers in the Bill, from among Australia's counterparts in the Five Eyes alliance, concerning the existence and scope of powers, and authorisation requirements.

Question 1 Issuing authorities for existing electronic surveillance warrants

2. The information referred to during the hearing about issuing authorities for existing surveillance device and telecommunications interception warrants is provided at **Attachment 1**. Please also see page 132, paragraph 482 of the Law Council's submission to the Committee's review of the present Bill.

3. Attachment 1 contains responses by the AAT to two questions on notice from the Senate Legal and Constitutional Affairs Legislation Committee in February 2020, as part of the 2019-20 Senate Estimates process. It provides statistical data from the AAT's records about the time taken by AAT members, while acting as issuing authorities, to determine applications for warrants under the *Surveillance Devices Act 2004* (Cth) (**SDA**) and *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), which would include applications made by the Australian Federal Police (**AFP**) and Australian Criminal Intelligence Commission (**ACIC**).

4. The AAT's records of unaudited data indicated that, since 1 July 2015, the average length of time spent on warrant applications under the SDA was 24 minutes, and 18 minutes for warrant applications under the TIA Act. The shortest recorded length of time for warrant applications under both Acts was one minute.[1]

[1] AAT, *Responses to Senate Legal and Constitutional Affairs Committee Questions on Notice 163 and 201*, Additional Estimates Hearings, 5 February 2020. (See responses to sub-questions 14 and 15.)

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

Question 2 International comparators with the proposed powers in the Bill

5. In short, the Law Council is not aware of any other jurisdiction in the Five Eyes alliance that has conferred powers on its law enforcement agencies which are directly equivalent, or closely comparable, to the proposals in the Bill.

6. The closest, but inexact, comparator appears to be with the United Kingdom (**UK**), in respect of the proposed data disruption powers in Schedule 1 to the Bill. The following is a summary of this comparative analysis, including extracts and analysis of relevant comments of the Richardson Review on international comparators.

7. **Attachment 2** provides further details of the Law Council's review of relevant legislation of each of the Five Eyes jurisdictions, which highlights the absence of directly equivalent powers in those countries.

'Equipment interference warrants' in the UK

8. Under Part 5 of the *Investigatory Powers Act 2016* (UK) (**IPA**), the Metropolitan Police may obtain 'equipment interference warrants' that authorise 'interference' with electronic equipment for the purpose of preventing or detecting serious crime.[2] However, there are extensive differences in the activities authorised, the issuing process, and applicable review mechanisms.

9. In particular, the UK's equipment interference warrants only authorise 'interference' with electronic equipment (such as bypassing security measures applied to data held in a computer) for the purpose of obtaining communications content, data or any other information. They do not authorise interference for the purpose of actively and covertly frustrating the commission of a suspected offence.[3] Rather, the collection of content, data or other information is for the purpose of investigating and potentially prosecuting a suspected offence, or taking other enforcement or preventive action under separate sources of legal authority (such as seeking criminal asset confiscation orders, or exercising preventive terrorism-related powers). As such, the warrant-based equipment interference powers available to UK law enforcement under the IPA are more akin to Australian law enforcement agencies' powers under computer access warrants in existing Division 4 of Part 2 of the SDA.

10. Moreover, the UK's equipment interference warrants are subject to the 'double lock' issuing process, under which the issuing decisions of the Secretary of State for the Home Department are subject to review by Judicial Commissioners appointed to the Investigatory Powers Commission (who must be serving or retired judges of superior courts).[4]

11. The issuing criteria for the UK's equipment interference warrants also include specific thresholds of necessity and proportionality.[5] Explicit thresholds and limitations apply to categories of particularly sensitive information, including legally privileged information and confidential journalistic information.[6] The application and execution of warrants is also governed by a binding Code of Practice made under the IPA, which provides detailed guidance on implementing the relevant statutory requirements.[7]

12. The UK Investigatory Powers Tribunal can review the legality of equipment interference warrants and actions taken in purported compliance with warrants, both

[2] IPA (UK), paragraphs 102(1)(a) and 106(1)(a).
[3] Ibid, subsection 99(2).
[4] Ibid, sections 102 and 108.
[5] Ibid, paragraphs 106(1)(a) and (b)
[6] Ibid, sections 111-114 and 131.
[7] Ibid, section 214 and Schedule 7; and Home Office (UK), *Equipment Interference: Code of Practice Pursuant to Schedule 7 to the Investigatory Powers Act 2016*, (March 2018).

under the IPA itself and the *Human Rights Act 1998* (UK).[8] This is supplemented by special procedures for managing operationally sensitive information, including proceeding on the basis of 'assumed facts' without requiring agencies to confirm or deny the existence of sensitive operations or other confidential matters.[9]

13. The IPA also establishes an 'error reporting' mechanism, whereby the Investigatory Powers Commissioner must disclose to affected persons serious errors by investigatory agencies in the exercise of investigatory powers, which have caused serious prejudice to the interests of the affected persons. This is provided that the Commissioner considers that disclosure is in the public interest, having regard to countervailing considerations of potential prejudice to security arising from disclosure. This notification mechanism enables affected individuals to pursue legal remedies for any serious loss, damage or harm caused by the activities of investigatory agencies, while also protecting highly sensitive information.[10]

'Criminal conduct authorisations' for certain undercover operations

14. In January 2021, the UK Parliament passed the *Covert Human Intelligence Sources (Criminal Conduct) Act 2021* (UK), which amended Part II of the *Regulatory Powers Act 2000* (UK) (**RIPA**) to establish a statutory process for authorising and immunising conduct that would otherwise be criminal, as part of an undercover operation by a law enforcement or intelligence agency that involves the use of a human source (which must also be separately approved under the RIPA). This is broadly comparable to Australia's controlled operations regime, which is available to the AFP and ACIC under Part IAB of the *Crimes Act 1914* (Cth) (**Crimes Act**).

15. The UK legislation commenced on 1 March 2021. It enables a public authority, including a police force, to obtain an internal authorisation, which enables officers or human sources to engage in criminal conduct in the course of, or otherwise in connection with, the conduct of covert human intelligence sources, for the purpose of for the purpose of 'preventing or detecting crime or of preventing disorder'.[11]

16. Criminal conduct authorisations are subject to express statutory issuing criteria of necessity and proportionality, including an explicit requirement to consider and exclude the possibility that the stated objective could be achieved through means other than criminal conduct, as well as complying with any further directions given by the Secretary of State for the Home Department.[12] These authorisations are not subject to external approval. However, they are subject to requirements to notify a Judicial Commissioner of the Investigatory Powers Commission of the issuance of an authorisation.[13] They are also subject to the oversight of the Investigatory Powers Commissioner, and review by the Investigatory Powers Tribunal, both under the RIPA and the *Human Rights Act 1998* (UK).[14]

17. On the face of the new provisions of the RIPA, criminal conduct authorisations appear capable of authorising data disruption activities in the context of a covert law enforcement operation relating to cyber-enabled crime that involves the use of a covert human source. This is provided that the disruption activity is necessary for, and proportionate to, the purpose of preventing crime. However, the Law Council has

[8] Ibid, section 243. See also: *Regulation of Investigatory Powers Act 2000* (UK), paragraph 65(2)(a).
[9] *Regulation of Investigatory Powers Act 2000* (UK), sections 68 and 69; and *Investigatory Powers Tribunal Rules 2000* (UK), rule 6(1). See also: Investigatory Powers Tribunal, Closed and Open Procedures, <https://www.ipt-uk.com/content.asp?id=13>.
[10] IPA, section 231.
[11] RIPA, section 29B.
[12] Ibid, subsection 29B(4).
[13] Ibid, sections 32C.
[14] Ibid, section 65; and IPA, subsections 229(4A)-(4C).

not identified official information on the public record that either confirms or denies the actual or intended use of the powers in this manner.

Domestic disruption powers of the UK's signals intelligence agency

18. Separately to the equipment interference powers in the IPA and criminal conduct authorisations in connection with covert operations, the UK's signals intelligence agency, the Government Communications Headquarters (**GCHQ**), is conferred with offensive powers to disrupt cybercrime both within and outside the UK.

19. Under section 5 of the *Intelligence Services Act 1994* (UK), GCHQ may obtain ministerially-issued warrants authorising the agency to undertake offensive cyber activities. However, these warrants are subject to explicit issuing tests of necessity and proportionality.[15] Further, in January 2021, the High Court of England and Wales held that these warrants must specifically identify the persons and property which are to be the subject of the relevant powers. These warrants cannot be issued in terms so broad that they effectively devolve decisions about the persons and property within scope to the discretion of the officials executing a warrant. The High Court held that warrants will be invalid if they purport to do so.[16]

20. It should also be noted that, like investigatory warrants under the IPA, decisions about the issuance and execution of warrants under the *Intelligence Services Act 1994* (UK) are challengeable by way of complaint to the Investigatory Powers Tribunal under the *Regulation of Investigatory Powers Act 2000* (UK), or the *Human Rights Act 1998* (UK).[17] Decisions of the Investigatory Powers Tribunal are judicially reviewable.[18]

21. In contrast to GCHQ, the functions of the Australian Signals Directorate (**ASD**) under paragraph 7(1)(c) of the *Intelligence Services Act 2001* (Cth) are limited to the prevention and disruption of cybercrime undertaken by entities outside Australia. (This is consistent with the fact that the functions of ASD have always been directed to the activities, intentions and capabilities of persons outside Australia.)

Richardson Review comments on differences between UK & Australian approaches

22. The Richardson Review considered that the availability of domestic data disruption powers in the UK, under warrants issued to GCHQ pursuant to the *Intelligence Services Act 1994* (UK), represented an historical practice in the drafting of that agency's statutory functions, which did not contain territorial application provisions that distinguished between GCHQ's 'onshore' or 'offshore' activities.[19] The Richardson Review emphasised that this had not been the practice in Australia, and as such, it would be a 'profound change' to confer explicit 'onshore' disruption powers that are exercisable within Australia's territorial jurisdiction, with any such proposals requiring a compelling justification of their necessity.[20]

23. The Richardson Review was unable to comment on the criminal conduct authorisation legislation in the UK, as it was introduced and passed after the Review was completed. However, the Richardson Review noted that the Australian controlled operations regime in the Crimes Act was one of the sources of statutory authority presently available to Australian law enforcement agencies for the purpose of

---

[15] *Intelligence Services Act 1994* (UK), paragraphs 5(2)(a) and (b).
[16] *Privacy International v Investigatory Powers Tribunal* [2021] EWHC 27 (Admin) (8 January 2021).
[17] *Regulation of Investigatory Powers Act 2000* (UK), section 65.
[18] *R (on the application of Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22 (15 May 2019), in which a purported ouster clause was read down to cover only matters going to the Tribunal's jurisdiction.) See further: IPA, section 242 (statutory rights of appeal in relation to certain Tribunal decisions, which came into effect in December 2018).
[19] Richardson Review, *Unclassified Report,* Vol 3, (December 2019), 218 at [38.55].
[20] Ibid.

disrupting cyber-enabled crime, even if no prosecution is possible at the end of the relevant criminal investigation, of which the controlled operation formed part.[21]

24. The Law Council concurs with the strong caution sounded by the Richardson Review against assuming that the present absence of explicit, domestic powers of data disruption amounts to a legislative gap that requires filling. As the Richardson Review observed, contentions that there are unintended gaps or other limitations in existing statutory powers require careful scrutiny.[22] The Richardson Review's assessment, based on its examination of agency submissions to that Review, was that 'very often such claims do not withstand even modest inquiry', and that some proposals advanced by agencies to the Review amounted to 'little more than a bid to expand functions and powers' without an adequate understanding of the fact that the limitations in existing statutory powers were imposed deliberately, to serve as 'guardians of valuable principles'.[23]

25. Following an assessment of the case advanced by agencies for specific 'onshore' disruption powers, the Richardson Review concluded that the absence of such powers did not constitute a legislative gap in existing powers, which necessitated the conferral of an explicit, domestic 'offensive' cybersecurity power on any Australian agency (whether a law enforcement or an intelligence agency). Rather, the Richardson Review recommended that ASD's disruption functions should remain limited to cybercrime occurring outside Australia. It further considered that domestic law enforcement agencies, principally the AFP, should continue to make use of their existing powers to engage in disruption activities (such as via controlled operations), and their existing powers to investigate and enforce offences (such as under computer access and surveillance device warrants), while also enhancing their technical disruption capabilities, with the technical assistance of ASD as necessary.[24]

26. The Law Council is concerned that the limited information provided in the extrinsic materials to the Bill does not provide a clear or cogent basis for the proposed departure from the Richardson Review's recommendation—which identified, and supported the retention of, a principled distinction between the approaches taken in Australia and the UK. The Law Council emphasises three key gaps in the justification provided in the extrinsic materials to the Bill and unclassified agency submissions:

- ***existing powers to carry out data disruption***—no particulars are 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;

- ***gaps in the case for the proportionality of data disruption powers***—the Law Council cautions against giving weight to suggestions that the Richardson Review recommendation should be disregarded, because the Bill proposes to authorise the disruption of data, and would exclude acts which cause permanent loss of property, money or digital currency.[25] In fact, the Bill will permit the AFP and ACIC to engage in acts of data disruption which have the following, serious impacts, if the officers executing the warrant self-assess those impacts to be 'justified and proportionate':[26]

    - acts of data disruption that cause major losses of future income to lawful computer users, as they are unable to conduct their online business; and

[21] Ibid, 219 at [38.64].
[22] Richardson Review, *Unclassified Report*, Volume 1 (December 2019), 34-35 at [3.12]-[3.15] and [3.19].
[23] Ibid, 35 at [3.19].
[24] Ibid, *Unclassified Report*, Volume 3 ,(December 2019), 218-221 at [38.58]-[38.76] and rec 162.
[25] Bill, Schedule 1, item 13 (inserting proposed paragraph 27KE(12)(b) of the SDA).
[26] Ibid, Schedule 1, item 13 (inserting proposed paragraph 27KE(7)(b) of the SDA).

- acts that do not destroy physical computer hardware, but significantly impair its functionality for a prolonged period of time, thereby 'hollowing out' the value of ownership or usage rights in the physical property; and

- ***ability to use existing investigatory warrants***—the extrinsic materials to the Bill contend that all three new warrant-based powers in the Bill are needed because of technological difficulties in identifying and locating suspects, and particularising their cyber-enabled offending at the early stages of an investigation.[27] However, they do not acknowledge or explain perceived limitations in the following, existing powers:

  - the explicit power in subparagraph 27A(1)(c)(ii) of the SDA to obtain and execute a computer access warrant for the purpose of identifying and locating a suspect in relation to the specified offence or offences (not merely investigating the conduct comprising the offences); and

  - the power in section 27F of the SDA to obtain variations to computer access warrants, to add further suspected 'relevant offences' that may be identified as an investigation progresses (and the ability for a cybercrime investigation to be supported by multiple, concurrent computer access warrants, which collectively cover all relevant offences). If the underlying issue is, in fact, one of operational efficiency or convenience rather than a lack of power, it is important that this is acknowledged and scrutinised.

Further information

27. Please contact Dr Natasha Molt, Director of Policy, on (02) 6246 3754 or natasha.molt@aph.gov.au if the Law Council may be of further assistance to the Committee in completing its review of the Bill.

Yours sincerely

Dr Jacoba Brasch QC
President

[27] Explanatory Memorandum, 2 at [2]-[4]. See also: the Hon Peter Dutton MP, Minister for Home Affairs, Second Reading Speech, SLAID Bill, (3 December 2020), *House of Representatives Hansard*, 10431-10432.

Question on notice no. 163

Portfolio question number: 164

Supplementary budget estimates

Legal and Constitutional Affairs Committee, Attorney-General's Portfolio

Senator the Hon. Kim Carr: asked the Administrative Appeals Tribunal on 22 October 2019—

(1. In respect of each year between 2015/16 to 2018/19, how many warrants under the Surveillance Devices Act 2004 were
issued by AAT Members? What type of warrants did they issue?
2. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 across the country:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
3. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in NSW:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
4. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Victoria:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
5. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Tasmania:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
6. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Western Australia:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?

7. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Queensland:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
8. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in the ACT:a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
9. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in South Australia:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
10. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in the NT:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
11. In respect of each AAT Member who is currently authorised to issue warrants under the Surveillance Devices Act 2004:
a. What is his / her name?
b. Is he or she:
i. enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a
State or of the Australian Capital Territory; and
ii. has been so enrolled for not less than 5 years?
c. How many warrants under the Surveillance Devices Act 2004 did he or she issue in 2016/17?
d. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse in 2016/17?
e. How many warrants under the Surveillance Devices Act 2004 did he or she issue in 2017/18?
f. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse in 2017/18;
g. How many warrants under the Surveillance Devices Act 2004 did he or she issue in 2018/19?
h. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse in 2018/19?

i. How many warrants under the Surveillance Devices Act 2004 did he or she issue between 1 July 2019 and the
present?
j. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse between 1 July
2019 and the present?
12. In respect of every Member who was authorised to issue warrants under the Surveillance Devices Act 2004 between 1 July
2015 and the present but who was not enrolled as a legal practitioner for at least 5 years:
a. what is / was his or her name;
b. how many warrants did he or she issue over the relevant period; and
c. how many applications for an interception warrant did he or she refuse over the relevant period?
13. In respect of each year between 2013/14 to 2018/19, how many times did an AAT Member refuse an application for a
warrant under the Surveillance Devices Act 2004?
14. Since 1 July 2015, what is the average amount of time it takes an AAT Member to consider an application for a warrant
under the Surveillance Devices Act 2004?
15. Since 1 July 2015, what is the shortest amount of time it has ever taken an AAT Member to consider an application for a
warrant under the Surveillance Devices Act 2004?
16. Having regard to paras 1.11, 7.26 and 10.23 of the recent report by the Hon. Ian Callinan AC into the Administrative
Appeals Tribunal, since 1 July 2015:a. Has a Member of the AAT ever sought, or received, legal advice from an AAT staff member in respect of an
application for a warrant under the Surveillance Devices Act 2004?
b. If so:
i. How many times did a Member of the AAT seek legal advice from an AAT staff member in respect of an
application for a warrant under the Surveillance Devices Act 2004?
ii. How many times did a Member of the AAT receive legal advice from an AAT staff member in respect of an
application for a warrant under the Surveillance Devices Act 2004?
c. Are there any "templates" used by AAT Members in relation to applications for warrants under the Surveillance
Devices Act 2004? Please provide the Committee with copies of all relevant templates.
17. Has a Member of the AAT ever asked an AAT staff member to prepare a decision, or to review and amend a draft decision,
in relation to a warrant application under the Surveillance Devices Act 2004? Please provide details.
Answer —
Please see the attached answer.

SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

ATTORNEY-GENERAL'S PORTFOLIO

SUPPLEMENTARY BUDGET ESTIMATES 2019-20

PA-Administrative Appeals Tribunal

LCC-SBE19-203 - Warrants under the Surveillance Devices Act 2004 Issued by the AAT

Senator Kim Carr asked the following question on 4 November 2019:

1. In respect of each year between 2015/16 to 2018/19, how many warrants under the Surveillance Devices Act 2004 were issued by AAT Members? What type of warrants did they issue?
2. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 across the country:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
3. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in NSW:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
4. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Victoria:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
5. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Tasmania:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
6. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Western Australia:
a. as at 1 July 2016;
b. as at 1 July 2017;

c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
7. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in Queensland:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
8. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in the ACT:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
9. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in South Australia:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
10. How many AAT Members were authorised to issue warrants under the Surveillance Devices Act 2004 in the NT:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
11. In respect of each AAT Member who is currently authorised to issue warrants under the Surveillance Devices Act 2004:
a. What is his / her name?
b. Is he or she:
i. enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and
ii. has been so enrolled for not less than 5 years?
c. How many warrants under the Surveillance Devices Act 2004 did he or she issue in 2016/17?
d. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse in 2016/17?
e. How many warrants under the Surveillance Devices Act 2004 did he or she issue in 2017/18?
f. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse in 2017/18;
g. How many warrants under the Surveillance Devices Act 2004 did he or she issue in 2018/19?
h. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse in 2018/19?

i. How many warrants under the Surveillance Devices Act 2004 did he or she issue between 1 July 2019 and the present?
j. How many applications for a warrant under the Surveillance Devices Act 2004 did he or she refuse between 1 July 2019 and the present?
12. In respect of every Member who was authorised to issue warrants under the Surveillance Devices Act 2004 between 1 July 2015 and the present but who was not enrolled as a legal practitioner for at least 5 years:
a. what is / was his or her name;
b. how many warrants did he or she issue over the relevant period; and
c. how many applications for an interception warrant did he or she refuse over the relevant period?
13. In respect of each year between 2013/14 to 2018/19, how many times did an AAT Member refuse an application for a warrant under the Surveillance Devices Act 2004?
14. Since 1 July 2015, what is the average amount of time it takes an AAT Member to consider an application for a warrant under the Surveillance Devices Act 2004?
15. Since 1 July 2015, what is the shortest amount of time it has ever taken an AAT Member to consider an application for a warrant under the Surveillance Devices Act 2004?
16. Having regard to paras 1.11, 7.26 and 10.23 of the recent report by the Hon. Ian Callinan AC into the Administrative Appeals Tribunal, since 1 July 2015:
a. Has a Member of the AAT ever sought, or received, legal advice from an AAT staff member in respect of an application for a warrant under the Surveillance Devices Act 2004?
b. If so:
i. How many times did a Member of the AAT seek legal advice from an AAT staff member in respect of an application for a warrant under the Surveillance Devices Act 2004?
ii. How many times did a Member of the AAT receive legal advice from an AAT staff member in respect of an application for a warrant under the Surveillance Devices Act 2004?
c. Are there any "templates" used by AAT Members in relation to applications for warrants under the Surveillance Devices Act 2004? Please provide the Committee with copies of all relevant templates.
17. Has a Member of the AAT ever asked an AAT staff member to prepare a decision, or to review and amend a draft decision, in relation to a warrant application under the Surveillance Devices Act 2004? Please provide details.

The response to the honourable senator's question is as follows:

Members of the AAT who meet the eligibility requirements may be nominated by the Attorney-General to be a nominated AAT member under section 13 of the *Surveillance Devices Act 2004* (the Act) to issue surveillance device warrants, retrieval warrants and computer access warrants, or exercise related powers. Members undertake these functions in a personal capacity (as a persona designata) and not as part of their duties as a member of the AAT. The AAT and AAT staff provide limited assistance to facilitate the performance of these functions, particularly scheduling appointments.

1. This question should be directed to the Department of Home Affairs which administers the Act.

2.-10. The following table sets out information derived from records held by the AAT about the number of AAT members who were nominated AAT members under the Act at the dates specified in the first column.

	ACT	NSW	NT	Qld	SA	Tas	Vic	WA	Total
At 1 July 2016	2	9	0	2	2	3	5	3	**26**
At 1 July 2017	2	12	0	3	3	3	6	2	**31**
At 1 July 2018	1	11	0	5	4	3	5	3	**32**
At 1 July 2019	2	11	0	4	4	2	6	3	**32**
At 31 October 2019	2	11	0	4	4	2	6	3	**32**

11.a. The names of AAT members who are nominated AAT members under the Act are not publicly disclosed. The issue of warrants for law enforcement purposes and the exercise of related powers, particularly in relation to the investigation of serious offences, gives rise to potential risks to the safety of persons undertaking these functions. Public disclosure of their identity may affect the willingness of eligible AAT members to consent to perform the functions and prejudice the maintenance of lawful methods for the protection of public safety. In these circumstances, it would contrary to the public interest to disclose the information publicly.

11. b. The AAT's records indicate that all but one of the AAT members who were nominated AAT members under the Act as at 4 November 2019 have advised that they are enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory and have been so enrolled for not less than 5 years.

11. c.–j. This request should be directed to the Department of Home Affairs which administers the Act.

12. a. The AAT's records indicate that only one AAT member has been a nominated AAT member under section 13 of the Act between 1 July 2015 and 4 November 2019 who did not advise that he was enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory. The names of nominated AAT members under the Act are not publicly disclosed for the reasons set out in the response to question 11.a.

12. b.–c. These questions should be directed to the Department of Home Affairs which administers the Act

13. This question should be directed to the Department of Home Affairs which administers the Act.

14.–15. The AAT's records do not allow the AAT to identify specifically the amount of time taken to consider an application for a warrant under this Act. The AAT records information about the duration of appointments held with an AAT member for the purposes of a persona designata function at which a member may:

- consider an application for the issue of a warrant or for an extension or variation of a warrant that has been issued;
- give further consideration to an application in relation to which additional information has been requested; or
- deal with an administrative matter arising in relation to a warrant.

The average (mean) length of all appointments held since 1 July 2015, for any purpose, that are recorded as relating to an application under this Act is 24 minutes. The shortest amount of time recorded for an appointment that proceeded is 1 minute. The data is not subject to auditing.

16. a.–b. Applications made under the Act are dealt with exclusively by the AAT member in confidence in accordance with the requirements of the Act. AAT staff do not provide any legal support in respect of applications considered by an AAT member under the Act.

16. c. The AAT does not make any templates available to members to use in relation to applications under the Act.

17. See the response to question 16. a.

Question on notice no. 201

Portfolio question number: 202

Supplementary budget estimates

Legal and Constitutional Affairs Committee, Attorney-General's Portfolio

Senator the Hon. Kim Carr: asked the Administrative Appeals Tribunal on 4 November 2019—

1. In respect of each year between 2015/16 to 2018/19, how many warrants under the *Telecommunication (Interception and Access) Act 1979* were issued by AAT Members? What type of warrants did they issue?

2. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* across the country:

    a. as at 1 July 2016;

    b. as at 1 July 2017;

    c. as at 1 July 2018;

    d. as at 1 July 2019; and

    e. as at 31 October 2019?

3. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in NSW:

    a. as at 1 July 2016;

    b. as at 1 July 2017;

    c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

4. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in Victoria:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

5. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in Tasmania:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

6. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in Western Australia:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

7. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in Queensland:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

8. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in the ACT:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

9. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in South Australia:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

10. How many AAT Members were authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* in the NT:

a. as at 1 July 2016;

b. as at 1 July 2017;

c. as at 1 July 2018;

d. as at 1 July 2019; and

e. as at 31 October 2019?

11. In respect of each AAT Member who is currently authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979*:

a. What is his / her name?

b. Is he or she:

i. enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and

ii. has been so enrolled for not less than 5 years?

c. How many warrants under the *Telecommunication (Interception and Access) Act 1979* did he or she issue in 2016/17?

d. How many applications for a warrant under the *Telecommunication (Interception and Access) Act 1979* did he or she refuse in 2016/17?

e. How many warrants under the *Telecommunication (Interception and Access) Act 1979* did he or she issue in 2017/18?

f. How many applications for a warrant under the *Telecommunication (Interception and Access) Act 1979* did he or she refuse in 2017/18;

g. How many warrants under the *Telecommunication (Interception and Access) Act 1979* did he or she issue in 2018/19?

h. How many applications for a warrant under the *Telecommunication (Interception and Access) Act 1979* did he or she refuse in 2018/19?

i. How many warrants under the *Telecommunication (Interception and Access) Act 1979* did he or she issue between 1 July 2019 and the present?

j. How many applications for a warrant under the *Telecommunication (Interception and Access) Act 1979* did he or she refuse between 1 July 2019 and the present?

12. In respect of every Member who was authorised to issue warrants under the *Telecommunication (Interception and Access) Act 1979* between 1 July 2015 and the present but who was not enrolled as a legal practitioner for at least 5 years:

a. what is / was his or her name;

b. how many warrants did he or she issue over the relevant period; and

c. how many applications for an interception warrant did he or she refuse over the relevant period?

13. In respect of each year between 2013/14 to 2018/19, how many times did an AAT Member refuse an application for a warrant under the *Telecommunication (Interception and Access) Act 1979*?

14. Since 1 July 2015, what is the average amount of time it takes an AAT Member to consider an application for a warrant under the *Telecommunication (Interception and Access) Act 1979*?

15. Since 1 July 2015, what is the shortest amount of time it has ever taken an AAT Member to consider an application for a warrant under the *Telecommunication (Interception and Access) Act 1979*?

1. Having regard to paras 1.11, 7.26 and 10.23 of the recent report by the Hon. Ian Callinan AC into the Administrative Appeals Tribunal, since 1 July 2015:

a. Has a Member of the AAT ever sought, or received, legal advice from an AAT staff member in respect of an application for a warrant under the *Telecommunication (Interception and Access) Act 1979*?

b. If so:

i. How many times did a Member of the AAT seek legal advice from an AAT staff member in respect of an application for a warrant under the *Telecommunication (Interception and Access) Act 1979*?

ii. How many times did a Member of the AAT receive legal advice from an AAT staff member in respect of an application for a warrant under the *Telecommunication (Interception and Access) Act 1979*?

c. Are there any “templates” used by AAT Members in relation to applications for warrants under the *Telecommunication (Interception and Access) Act 1979*? Please provide the Committee with copies of all relevant templates.

2. Has a Member of the AAT ever asked an AAT staff member to prepare a decision, or to review and amend a draft decision, in relation to a warrant application under the *Telecommunication (Interception and Access) Act 1979*? Please provide details.

Answer —

Please see the attached answer.

SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

ATTORNEY-GENERAL'S PORTFOLIO

SUPPLEMENTARY BUDGET ESTIMATES 2019-20

PA-Administrative Appeals Tribunal

LCC-SBE19-165 - Warrants under the Telecommunication (Interception and Access) Act 1979 Issued by the AAT

Senator Kim Carr asked the following question on 04 November 2019:

1. In respect of each year between 2015/16 to 2018/19, how many warrants under the Telecommunication (Interception and Access) Act 1979 were issued by AAT Members? What type of warrants did they issue?
2. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 across the country:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
3. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in NSW:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
4. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in Victoria:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
5. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in Tasmania:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
6. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in Western Australia:
a. as at 1 July 2016;

b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
7. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in Queensland:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
8. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in the ACT:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
9. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in South Australia:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
10. How many AAT Members were authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 in the NT:
a. as at 1 July 2016;
b. as at 1 July 2017;
c. as at 1 July 2018;
d. as at 1 July 2019; and
e. as at 31 October 2019?
11. In respect of each AAT Member who is currently authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979:
a. What is his / her name?
b. Is he or she:
i. enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and
ii. has been so enrolled for not less than 5 years?
c. How many warrants under the Telecommunication (Interception and Access) Act 1979 did he or she issue in 2016/17?
d. How many applications for a warrant under the Telecommunication (Interception and Access) Act 1979 did he or she refuse in 2016/17?
e. How many warrants under the Telecommunication (Interception and Access) Act 1979 did he or she issue in 2017/18?
f. How many applications for a warrant under the Telecommunication (Interception and Access) Act 1979 did he or she refuse in 2017/18;
g. How many warrants under the Telecommunication (Interception and Access) Act 1979 did he or she issue in 2018/19?
h. How many applications for a warrant under the Telecommunication (Interception and

Access) Act 1979 did he or she refuse in 2018/19?
i. How many warrants under the Telecommunication (Interception and Access) Act 1979 did he or she issue between 1 July 2019 and the present?
j. How many applications for a warrant under the Telecommunication (Interception and Access) Act 1979 did he or she refuse between 1 July 2019 and the present?
12. In respect of every Member who was authorised to issue warrants under the Telecommunication (Interception and Access) Act 1979 between 1 July 2015 and the present but who was not enrolled as a legal practitioner for at least 5 years:
a. what is / was his or her name;
b. how many warrants did he or she issue over the relevant period; and
c. how many applications for an interception warrant did he or she refuse over the relevant period?
13. In respect of each year between 2013/14 to 2018/19, how many times did an AAT Member refuse an application for a warrant under the Telecommunication (Interception and Access) Act 1979?
14. Since 1 July 2015, what is the average amount of time it takes an AAT Member to consider an application for a warrant under the Telecommunication (Interception and Access) Act 1979?
15. Since 1 July 2015, what is the shortest amount of time it has ever taken an AAT Member to consider an application for a warrant under the Telecommunication (Interception and Access) Act 1979?
16. Having regard to paras 1.11, 7.26 and 10.23 of the recent report by the Hon. Ian Callinan AC into the Administrative Appeals Tribunal, since 1 July 2015:
a. Has a Member of the AAT ever sought, or received, legal advice from an AAT staff member in respect of an application for a warrant under the Telecommunication (Interception and Access) Act 1979?
b. If so:
i. How many times did a Member of the AAT seek legal advice from an AAT staff member in respect of an application for a warrant under the Telecommunication (Interception and Access) Act 1979?
ii. How many times did a Member of the AAT receive legal advice from an AAT staff member in respect of an application for a warrant under the Telecommunication (Interception and Access) Act 1979?
c. Are there any "templates" used by AAT Members in relation to applications for warrants under the Telecommunication (Interception and Access) Act 1979? Please provide the Committee with copies of all relevant templates.
17. Has a Member of the AAT ever asked an AAT staff member to prepare a decision, or to review and amend a draft decision, in relation to a warrant application under the Telecommunication (Interception and Access) Act 1979? Please provide details.

The response to the honourable senator's question is as follows:

Members of the AAT who meet the eligibility requirements set out in the *Telecommunications (Interception and Access) Act 1979* (the Act) may be nominated as a nominated AAT member or appointed as an issuing authority or a Part 4-1 issuing authority by the Attorney-General under section 6DA, 6DB or 6DC to issue:

- warrants authorising the interception of telecommunications under Part 2-5

- stored communications warrants under Part 3-3, or
- journalist information warrants under Part 4-1.

Members undertake these functions in a personal capacity (as a persona designata) and not as part of their duties as a member of the AAT. The AAT and AAT staff provide limited assistance to facilitate the performance of these functions, particularly scheduling appointments.

1. This question should be directed to the Department of Home Affairs which administers the Act.

2.–10. The following table sets out information derived from records held by the AAT about the number of AAT members who were either nominated AAT members, issuing authorities or Part 4-1 issuing authorities under the Act at the dates specified in the first column.

	ACT	**NSW**	**NT**	**Qld**	**SA**	**Tas**	**Vic**	**WA**	**Total**
At 1 July 2016	2	9	0	2	2	3	5	3	**26**
At 1 July 2017	2	12	0	3	3	3	6	2	**31**
At 1 July 2018	1	11	0	5	4	3	5	3	**32**
At 1 July 2019	2	11	0	4	4	2	6	3	**32**
At 31 October 2019	2	11	0	4	4	2	6	3	**32**

11. a. The names of AAT members who are nominated AAT members, issuing authorities or Part 4-1 issuing authorities under the Act are not publicly disclosed. The issue of warrants for law enforcement purposes, particularly in relation to the investigation of serious offences, gives rise to potential risks to the safety of persons undertaking these functions. Public disclosure of their identity may affect the willingness of eligible AAT members to consent to perform the functions and prejudice the maintenance of lawful methods for the protection of public safety. In these circumstances, it would contrary to the public interest to disclose the information publicly.

11. b. The AAT's records indicate that all but one of the AAT members who were nominated AAT members, issuing authorities or Part 4-1 issuing authorities under the Act as at 4 November 2019 have advised that they are enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory and have been so enrolled for not less than 5 years.

11. c.–j. These questions should be directed to the Department of Home Affairs which administers the Act.

12. a. The AAT's records indicate that only one AAT member has been a nominated AAT member under section 6DA of the Act between 1 July 2015 and 4 November 2019 who did not advise that he was enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory. The names of nominated AAT members, issuing authorities or Part 4-1 issuing authorities under the Act are not publicly disclosed for the reasons set out in the response to question 11.a.

12. b.–c. These questions should be directed to the Department of Home Affairs which administers the Act.

13. This question should be directed to the Department of Home Affairs which administers the Act.

14.–15. The AAT's records do not allow the AAT to identify the amount of time taken to consider an application for a warrant under this Act. The AAT records information about the duration of appointments held with an AAT member for the purposes of a persona designata function at which a member may:

- consider a new application for the issue of a warrant or a renewal application for a warrant still in force;
- give further consideration to an application in relation to which additional information has been requested; or
- deal with an administrative matter arising in relation to a warrant.

The average (mean) length of all appointments held since 1 July 2015, for any purpose, that are recorded as relating to an application under this Act is 18 minutes. The shortest amount of time recorded for an appointment that proceeded is 1 minute. The data is not subject to auditing.

16. a.–b. Applications made under the Act are dealt with exclusively by the AAT member in confidence in accordance with the requirements of the Act. AAT staff do not provide any legal support in respect of applications considered by an AAT member under the Act.

16. c. The AAT does not make any templates available to members to use in relation to applications under the Act.

17. See the response to question 16.a.

Law Council of Australia

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 ('SLAID Bill')

Summary of international comparators among the Five Eyes alliance, based on a desktop review of legislation at March 2021

1. Domestic data disruption powers

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
Australia	SLAID Bill, Schedule 1 (Inserting new Division 5 of Part 2 of the *Surveillance Devices Act 2004* (Cth) / **SDA**)	Australian Federal Police (**AFP**) Australian Criminal Intelligence Commission (**ACIC**)	**Data disruption warrants** Authorise the disruption of data for the purpose of frustrating the commission of a relevant offence specified in the warrant instrument.	**Applicant:** law enforcement officer of AFP or ACIC **Issuing authority:** 'eligible judge' (a judge of a federal court) or 'nominated AAT member' (an AAT member who has been admitted as an Australian lawyer for five more years) appointed by the Attorney-General.	• There are reasonable grounds for the suspicion founding the warrant (concerning the commission of relevant offences involving data held in a computer, and the likelihood that data disruption will substantially assist in frustrating the commission of relevant offences of the kind specified in the application). • Data disruption is reasonable and proportionate, having regard to the kinds of relevant offences referred to in the warrant application. • Must have regard to the matters in s 27KC(2) which are directed to some, but not all, of the considerations that are relevant to the proportionality of the proposed powers.

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
United Kingdom **<u>Summary:</u>** Similar data disruption powers under the *Intelligence Services Act 1994* (UK), but exercisable by the national signals intelligence agency under warrant, with stronger issuing criteria and rights of review. Law enforcement agencies are limited to the equivalent of Australia's computer access warrants, and controlled operations.	*Intelligence Services Act 1994* (UK), s 5	Government Communications Headquarters (**GCHQ**) – the UK signals intelligence agency	**Intelligence Services Act warrants** Authorise entry on, and interference with, property or wireless telegraphy, for the purpose of GCHQ carrying out any of its functions under s 3(1)(a) (monitoring, using and interference with electronic signals) for the purpose of preventing or detecting serious crime, national security, or the economic well-being of the UK. Warrants that authorise such activities on a domestic basis may only be issued for the purpose of preventing or detecting serious crime that either: (a) involves violence, results in substantial financial gain, or is conduct by a large number of persons in pursuit of a common purpose; or (b) the offence(s) are punishable by a maximum penalty of three years' imprisonment.	**Applicant:** GCHQ head or another person on their behalf. **Issuing authority:** Secretary of State for the Home Department. Issuing decisions are subject to review by the Investigatory Powers Tribunal, and Tribunal decisions are judicially reviewable (other than in relation to matters going to that Tribunal's jurisdiction): *Regulation of Investigatory Powers Act 2000* (UK), ss 65 and 68.	• Necessity and proportionality (including an assessment of the availability and effectiveness of alternative means) • Adequate measures are in place to protect against unauthorised disclosure or access, and retention of information beyond the permissible period. Note also that the decision in *Privacy International v Investigatory Powers Tribunal* [2021] EWHC 27 requires these warrants to specify, with sufficient particularity, the persons and property which are to be the subject of the relevant powers. A warrant will be invalid if it does not do so.

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
United Kingdom	*Investigatory Powers Act 2016* (UK) (**IPA**), Part 5 (equipment interference warrants) **Note:** these warrants authorise electronic surveillance only for investigatory purposes, not disruption for the purposes of frustrating an offence. They are more akin to the AFP and ACIC's computer access warrants in Div 4 of Pt 2 of the SDA.	Relevantly includes: • Metropolitan Police • National Crime Agency • Intelligence Services (MI5, MI6, GCHQ) (See further: IPA, s 106 and Schedule 6.)	**Equipment interference warrants** Authorise interference with electronic equipment for the purpose of obtaining communications, data or any other information. For law enforcement agencies, access must be for the purpose of preventing or detecting serious crime. For the intelligence services, access must be in the interests of national security; or preventing or detecting serious crime; or the interests of the UK's economic well-being, but only to the extent those interests are also relevant to national security interests. IPA, ss 99-107.	**Applicant:** agency head or a person acting on their behalf. **Issuing authority:** 'double lock' process: • The Secretary of State for the Home Department makes the issuing decision. • The warrant only takes effect once the issuing decision is approved on review by a Judicial Commissioner of the Investigatory Powers Commission (a serving or retired superior court judge). IPA, ss 102-110.	• Necessity and proportionality. • Adequate arrangements are in place to protect the information obtained against unauthorised access or disclosure, or retention beyond permissible period. • Additional requirements for privileged information (parliamentary and legal professional privilege) and journalistic materials. IPA, ss 102-107 and 111-114.
	Covert Human Intelligence Sources (Criminal Conduct) Act 2021 (UK), amending Part II of the *Regulation of Investigatory Powers Act 2000* (UK) (**RIPA**)	Relevantly includes: • Metropolitan Police • National Crime Agency • Intelligence Services (MI5, MI6, GCHQ) (See further: RIPA, ss 28-29 and Sch 1)	**Criminal conduct authorisations:** Authorise criminal conduct in the course of, or otherwise in connection with, the conduct of covert human intelligence sources, for the purpose of for the purpose of preventing	**Applicant and issuing authority:** internal within the relevant agency, subject to requirements to notify a Judicial Commissioner of the Investigatory Powers Commission. RIPA, s 29B.	• Necessity and proportionality. • Adequate arrangements are in place to satisfy requirements that may be set from time-to-time by the Secretary of State for the Home Department. • Additional requirements relating to investigations

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
			or detecting crime or of preventing disorder. RIPA, s 29B.		concerning children and vulnerable adults. RIPA, ss 29B, 29C and 29D.
United States **<u>Summary:</u>** No equivalent powers of domestic data disruption. Offensive cyber powers only appear to be conferred on the Department of Defence, and are limited to hostile foreign cyber operations. Law enforcement is limited to the equivalent of Australia's computer access warrants, with the ability to obtain a specific court order enabling a single warrant to allow remote access to a computer, irrespective of geographical location.	*Federal Rules of Criminal Procedure*, r 41 (made under 28 USC § 2072) **Note:** the FBI does not appear to have dedicated powers to covertly frustrate the commission of a cyber-enabled offence. Rather, the above rules enable a single search warrant to authorise remote computer access, irrespective of the geographical location of the target computer. This enables the FBI to disrupt cyber-enabled offending by exercising enforcement powers, such as arrest, where a suspect has used technology to obscure their identity, location and activities. As such, the FBI's powers are more closely analogous with the AFP and ACIC's existing computer access warrants in Div 4 of Part 2 of the SDA,	Federal Bureau of Investigation (**FBI**) **Note also**: the US Department of Defense has dedicated offensive cyber powers, but they are directed to military cyber security operations against hostile foreign cyber operations, <u>not</u> the criminal activities of non-state actors. These powers are exercisable for the purpose of '*defend[ing] the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power*': 10 USC, Chapter 19 (§ §393-397)	**Search warrants in relation to data held in a computer** A judge of a court in any district may issue a warrant to search a computer, irrespective of whether or not that computer is physically located in that district.	Judicial issuing. (Process is dependent on the individual statute conferring the underlying power of search.)	Dependent on the individual statute conferring the underlying power of search.

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
	and the definition of 'computer' in s 6.				
Canada **<u>Summary:</u>** Does not appear to have dedicated data disruption powers for law enforcement agencies, only the equivalent of Australia's controlled operations regime. Data disruption activities may be available to intelligence agencies, for security threat reduction purposes and offshore activities. In any event, subject to more stringent issuing criteria and process that the proposed regime of data disruption warrants for Australian law enforcement.	*Criminal Code,* R.S.C., 1985, c. C-46, s 25 (**Canadian Criminal Code**) **Note:** The RCMP does not appear to have specific data disruption powers. Some data disruption activities may be capable of authorisation under its equivalent regime to Australia's controlled operations (ie authority to commit what would otherwise be a criminal act).	Royal Canadian Mounted Police (**RCMP**)	**Criminal immunity—equivalent to Australia's controlled operations regime** An authorised officer is justified in committing an act or omission that would otherwise constitute an offence, if that officer is engaged in the investigation of criminal activity. Subject to limitations on conduct likely to cause loss of, or damage to, property. Canadian Criminal Code, s 25.1(8)	The relevant police officer must be authorised by the Minister of Public Safety and Emergency Preparedness (who is prescribed as the 'competent authority'). Canadian Criminal Code, ss 25.1(1) & (8).	The officer must believe, on reasonable grounds, that: *'the commission of the act or omission, as compared to the nature of the offence or criminal activity being investigated, is reasonable and proportional in the circumstances, having regard to such matters as the nature of the act or omission, the nature of the investigation and the reasonable availability of other means for carrying out the public officer's law enforcement duties'.* Canadian Criminal Code, s 25.1(8)(c).
	Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23 (**CSIS Act**) **Note:** CSIS does not appear to have specific data disruption powers. Some data disruption activities may be capable of authorisation under its 'security threat reduction powers'.	Canadian Security Intelligence Service (**CSIS**)	**Warrant-based threat reduction functions and powers** 'If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat': CSIS Act, s 12.1(1). Certain acts are expressly excluded, including acts causing loss or destruction of property if doing so	**Issuing authority:** If the proposed activity would limit a fundamental right or freedom under the Canadian Charter of Rights and Freedoms, it must be authorised by judicial warrant. **Applicant**: the head of CSIS or another member approved by the Minister. The application can only be made with the Minister's approval.	The judge can only issue the warrant if satisfied that the relevant threat reduction activities are reasonable, proportionate and compliant with the Canadian Charter of Rights and Freedoms. The judge can only authorise the activities specified in section 21.1(1.1) which include: *'(a) altering, removing, replacing, destroying, disrupting or degrading a communication or means of communication; and*

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
Canada	CSIS Act (ctd)	CSIS (ctd)	would endanger the safety of an individual. CSIS Act, ss 12.1(2) & (3.1), and s 12.2(1).	CSIS Act, ss 12.1(3.2)-(3.3) and 21.1(1).	*(b) altering, removing, replacing, destroying, degrading or providing — or interfering with the use or delivery of — any thing or part of a thing, including records, documents, goods, components and equipment'.* CSIS Act, ss 12.1 and 21.1(1).
	Communications Security Establishment Act, S.C. 2019, c. 13, s. 76 **Note:** The CSE's data disruption powers appear to be limited to offshore activities (which may include offshore cybercrime, to the extent it relates to international affairs, defence or security).	Communications Security Establishment (**CSE**)	**'Active cyber operations authorisations':** CSE may carry out, *'on or through the global information infrastructure, any activity specified in the authorization in the furtherance of the active cyber operations aspect of its mandate*': CSE Act, s 30(1). **Note**: the CSE's cyber operations mandate is *'to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security'*.	**Application:** CSE Chief **Issuing authority:** Minister of National Defence (with the approval of the Foreign Minister).	The Minister must be satisfied that: • *'there are reasonable grounds to believe that any activity that would be authorized by it is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities'*; and • *'the objective of the cyber operation could not reasonably be achieved by other means and that no information will be acquired under the authorization except in accordance with an authorization'.* CSE Act ss 34(1) and (4).

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
			They expressly exclude taking action inside Canada: CSE Act ss 19 and 22(2)(a).		
New Zealand **<u>Summary:</u>** Does not appear to have data disruption powers for law enforcement or intelligence agencies.	NZ intelligence and law enforcement agencies do not appear to have data disruption powers. Further, New Zealand Police do not appear to have a similar criminal immunity regime to Australia's controlled operations framework. However, in June 2017, the New Zealand Law Commission (**NZLC**) recommended the enactment of a statutory framework for controlled operations, in its review of the *Search and Surveillance Act 2012* (NZ). See: NZLC, Report 141, Chapter 15, especially p. 299 at [15.140]-[15.145] and recommendations R62 and R63.	N/A	N/A	N/A	N/A

2. Computer access powers for the purpose of criminal intelligence collection

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
Australia	SLAID Bill, Schedule 2 (inserting proposed Division 6 of Part 2 of the SDA)	AFP, ACIC	**Network activity warrants** Same powers as those available under computer access warrants. However the purpose of their exercise is the collection of intelligence in relation to a 'criminal network of individuals' rather than the investigation of a specified offence or offences.	Per table 1 above.	• There are reasonable grounds for the suspicion founding the warrant (namely, that access to the relevant data will substantially assist in the collection of intelligence about individuals in the criminal network, and is relevant to the prevention, detection or frustration of one or more kinds of relevant offences specified in the application). • Issuing authority must have regard to the matters specified in proposed s 27KM(2) which are directed to some, but not all, of the considerations that are relevant to an assessment of the proportionality of the proposed powers.
United Kingdom **<u>Summary:</u>** Powers available to law enforcement under the Part 5 of the IPA (equipment interference warrants) for the purpose of 'preventing or detecting' serious crime.	IPA, Part 5 (equipment interference warrants) *Intelligence Services Act 1994* (UK), s 5 (intelligence agencies only).	Per table 1 above.	Per table 1 above.	Per table 1 above.	Per table 1 above.

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
United States **Summary** The FBI has surveillance powers for intelligence purposes, but this recognises its fused security intelligence and law enforcement functions with respect to national security, including terrorism, in contrast to Australia.	*Foreign Intelligence Surveillance Act* (**FISA**) 50 USC §§1801-1813. *Federal Rules of Criminal Procedure*, Rule 41 (made under 28 USC § 2072).	FBI	Under the FISA, warrant-based electronic surveillance can be authorised for the purpose of gaining intelligence about international terrorism (being terrorism committed outside the US). However, targets may be in the US The Federal Rules of Criminal Procedure also enable a court order to approve the execution of a warrant (for example a search warrant issued under 18 USC Chapter 205), irrespective of the geographical location of a computer.	FISA warrants are issued by a dedicated court: FISA § 1805.	Under the FISA, the issuing judge must be satisfied that there is probably cause to believe that the target is a 'foreign power' or an 'agent of a foreign power' (including a person or group engaged in international terrorism); and that the facilities or places being targeted for surveillance are being used by the foreign power or agent; and that there are adequate minimisation procedures in place to prevent or limit access to and dissemination of information of US citizens. FISA § 1805.
Canada **Summary:** Law enforcement does not appear to have intelligence-collection powers.	RCMP does not appear to have dedicated criminal intelligence collection powers. The intelligence-collection powers of CSIS are directed to matters of security, which could cover conduct that also constitutes a cyber-enabled offence.	See left.	See left.	See left.	See left.
New Zealand **Summary:** Law enforcement does not appear to have	New Zealand law enforcement agencies do not appear to have warrant-based criminal	See left.	See left.	See left.	See left.

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
dedicated intelligence collection-powers.	intelligence collection powers. Intelligence collection powers are limited to the intelligence services, under the *Intelligence and Security Act 2017* (NZ) and would therefore only cover cyber-enabled crime if the relevant conduct was also a matter that was relevant to the protection of national security, international relations, and economic well-being.				

3. Online account takeover / 'lockout' powers

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
Australia	SLAID Bill, Schedule 3 Inserting new Part IAAC of the *Crimes Act 1914* (Cth)	AFP, ACIC	**Account takeover warrants** The power to take exclusive control of any online account, for the purpose of enabling evidence to be obtained of the commission of one or more relevant offences.	**Applicant:** any law enforcement officer of the AFP or ACIC. **Issuing authority**: a magistrate (acting in a personal capacity).	• There are reasonable grounds for the suspicion founding the warrant application. • The Magistrate must have regard to the matters specified in subsection 3ZZUP(2), which are directed to some, but not all, of the considerations that are relevant to an assessment of the proportionality of the proposed powers.
United Kingdom **<u>Summary:</u>** Does not have dedicated lockout powers, but may potentially be covered by GCHQ's intelligence warrants, or the equivalent of controlled operations by law enforcement.	Does not appear to have dedicated warrant-based powers directed to account takeover for investigative purposes. However, this may potentially be covered by a warrant issued to GCHQ under s 5 of the *Intelligence Services Act 1994* (Cth) to the extent that 'lockout' is considered to fall within the scope of GCHQ's interference functions in relation to the detection and prevention of serious crime. May also potentially be capable of authorisation under a 'criminal conduct authorisation'	Potentially GCHQ *(see caveat at left)*	Per tables 1 and 2 above.	Per tables 1 and 2 above.	Per tables 1 and 2 above.

Country	Powers available?	Agencies	Powers conferred: purpose & scope	Issuing process	Key issuing criteria
United Kingdom	given under section 29B of the RIPA (See table 1 above). However, the Law Council has not identified publicly available information, officially confirming or denying the any such the availability or use of these powers in such circumstances.				
United States **Summary:** No equivalent powers identified	Does not appear to have dedicated warrant-based powers directed to account takeover for investigative purposes.	N/A	N/A	N/A	N/A
Canada **Summary:** No equivalent powers identified. Potential that law enforcement may rely on authority under equivalent to Australia's controlled operations regime.	Does not appear to have dedicated warrant-based powers directed to account takeover for investigative purposes. Potentially able to be authorised under criminal immunity provisions in s 25 of the Canadian Criminal Code (See table 1). However, the Law Council has not identified publicly available information, officially confirming or denying the any such the availability or use of these powers in such circumstances.	See table 1 above.	See table 1 above.	See table 1 above.	See table 1 above.
New Zealand **Summary:** No equivalent powers identified	Does not appear to have dedicated warrant-based powers directed to account takeover for investigative purposes.	N/A	N/A	N/A	N/A