Law Council
OF AUSTRALIA

Australian Security Intelligence Organisation Amendment Bill 2020

Supplementary submission:

Parliamentary Joint Committee on Intelligence and Security

23 July 2020

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

Table of Contents

About the Law Council of Australia

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

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

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

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

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

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

Members of the 2020 Executive as at 1 January 2020 are:

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

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council gratefully acknowledges the assistance of its National Criminal Law Committee in the preparation of this supplementary submission.

Introduction

1. This submission supplements the Law Council's previous submissions and appearance before the Parliamentary Joint Committee on Intelligence and Security (**Committee**) on 10 July 2020.

2. The Committee is presently considering measures in Schedule 2 to the Bill, which would enable ASIO to self-authorise its use of tracking devices in certain circumstances, under a statutory application-based process in the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**).

3. The Law Council wishes to draw the Committee's attention to a further issue concerning these amendments. It arises from proposed subsection 33(4) of the ASIO Act, in item 16 of Schedule 2 to the Bill. The Law Council is concerned that, in some circumstances, this provision will apply to remove the obligation for the Australian Security Intelligence Organisation (**ASIO**) to obtain even a statutory internal authorisation to use a tracking device.

Proposed subsection 33(4) of the ASIO Act

4. Neither the existing provisions of the ASIO Act, nor the proposed amendments in the Bill, explicitly prohibit ASIO from installing, using, maintaining or recovering a tracking device, unless authorised under the ASIO Act. Rather, proposed subsection 33(4) (inserted by item 16 of Schedule 2 to the Bill) provides:

> *Nothing in this Division* [Division 2 of Part III – Special Powers] *makes the use, installation, maintenance or recovery by the Organisation of a surveillance device unlawful if the use, installation, maintenance or recovery would not otherwise be unlawful under any other applicable law of the Commonwealth, a State or a Territory (including the common law).*

Policy intent

5. The Explanatory Memorandum states that the purpose of the provision is to 'clarify' that ASIO is **not required** to 'obtain a warrant **or an internal authorisation** under Division 2 of Part III of the ASIO Act in circumstances where the conduct is not unlawful in the State or Territory in which it takes place (or under any applicable Commonwealth law or the common law)' (emphasis added).[1]

6. The submission of the Department of Home Affairs to the Committee states that proposed subsection 33(4) 'simply clarifies that, if it would be lawful for a member of the public to use a device, it is also lawful for ASIO to do so'.[2] This statement suggests a policy intention to align ASIO's authorisation requirements with the regulation of private individuals and bodies corporate under applicable Australian laws (which are principally State and Territory surveillance device laws).

7. However, this policy objective appears to overlook that the use of a surveillance device by an intelligence agency, such as ASIO, is likely to have a considerably greater impact on an individual's privacy than the use of such a device by a private individual or body corporate. This reflects the unique functions, substantial resourcing, and technical capability of an intelligence agency.

[1] Explanatory Memorandum, 132 at [718].
[2] Department of Home Affairs, *Submission to the Parliamentary Joint Committee on Intelligence and Security, Review of the ASIO Amendment Bill*, (May 2020), 49.

8. It also reflects the more extensive use that an intelligence agency may make of the intelligence collected, as distinct to a private person. For instance, it would be open to an intelligence agency to: combine the intelligence collected from the use of a surveillance device with other pieces of intelligence in its extensive holdings; disseminate this intelligence to domestic and foreign intelligence and law enforcement agencies; and use the intelligence collected from a surveillance device to obtain authorisations for intrusive collection powers against the target or others.

9. As explained below, the Law Council considers that the legal authorisation requirements for ASIO to use a surveillance device should reflect its unique status as an intelligence agency and an emanation of the State, rather than merely adopting the regulatory approach applicable to private persons as in existence from time-to-time. The Law Council considers it appropriate that ASIO is held to a higher standard than ordinary members of the public by reason of its status and functions.

10. As explained below, the *Intelligence Services Act 2001* (Cth) (**ISA**) already adopts this approach for the intelligence agencies governed by that Act. Those agencies are required to obtain a Ministerial authorisation to use a surveillance device on an Australian person. This requirement applies in all circumstances, even if the use of the surveillance device would not constitute an offence or tort under Australian law.[3]

Legal effect

11. The Law Council is concerned that proposed subsection 33(4) would allow ASIO to install and use a tracking device in a public place without **any kind** of statutory approval requirement in several States and Territories. This is provided that ASIO officers did not commit any offences or torts (such as assault, or trespass to goods or property) when installing, maintaining or using the tracking device.

12. There is considerable variation in individual State and Territory surveillance device laws. Based on the Law Council's examination of relevant legislation, it appears that, in the circumstances outlined in paragraph [11] above, ASIO **would be** required to obtain an internal authorisation under proposed section 26G of the ASIO Act to install, use, maintain and recover a tracking device in a public place in New South Wales,[4] Western Australia,[5] South Australia[6] and the Northern Territory.[7]

13. However, it appears that ASIO **would not** be required to obtain an internal authorisation under proposed section 26G of the ASIO Act in Victoria,[8] Queensland,[9] Tasmania[10] and the Australian Capital Territory.[11]

---

[3] ISA, sections 8 and 9, especially paragraph 8(1)(a)(i).
[4] *Surveillance Devices Act 2007* (NSW), section 9.
[5] *Surveillance Devices Act 1998* (WA), section 7.
[6] *Surveillance Devices Act 2016* (SA), section 7.
[7] *Surveillance Devices Act 2007* (NT), section 13.
[8] *Surveillance Devices Act 1999* (Vic), sections 8 (prohibition) and 5 (exclusion of ASIO officers from Act, including the general prohibition on the use of tracking devices unless authorised under an Australian law).
[9] Queensland legislation does not contain a general prohibition on the use of a tracking device: *Invasion of Privacy Act 1971* (Qld) (which only regulates listening devices) and *Police Powers and Responsibilities Act 2000* (Qld), Chapter 13 (which is limited to the use of surveillance devices by law enforcement agencies).
[10] Tasmanian legislation does not contain a general prohibition on the use of a tracking device. There is no general piece of legislation regulating surveillance devices by any person. The *Police Powers (Surveillance Devices) Act 2006* (Tas) is limited to law enforcement agencies.
[11] ACT legislation does not contain a general prohibition on the use of a tracking device. There is no general piece of legislation regulating surveillance devices by any person. The *Crimes (Surveillance Devices) Act 2010* (ACT) is limited to law enforcement agencies.

New South Wales, Western Australia, South Australia and the Northern Territory

14. The surveillance device legislation of these jurisdictions, cited in the footnotes to paragraph [12] above, contains a general prohibition on the use of a tracking device, unless authorised under those Acts or another law, including a law of the Commonwealth (such as the ASIO Act).

15. This means that ASIO would always be required to obtain at least an internal statutory authorisation to use a tracking device in these jurisdictions, so that it does not contravene the general prohibition in their surveillance device legislation.

16. If the actions involved in installing, using, maintaining or recovering the tracking device are excluded from a statutory internal authorisation under proposed section 26K, then ASIO would be required to obtain a surveillance device warrant under existing section 26.

17. Proposed section 26K excludes various activities that would otherwise involve the commission of an offence in the nature of trespass, or a computer offence. Namely: entering private premises or interfering with the interior of a vehicle without consent; remotely installing a tracking device, or doing other things for which ASIO would require a computer access warrant under section 25A, such as adding, copying or altering data; and using audio or optical surveillance capabilities on a device, in addition to tracking a person's location and movements.

Victoria, Queensland, Tasmania and the Australian Capital Territory

18. In Victoria, the *Surveillance Devices Act 1999* (Vic) contains a general prohibition on the use of tracking devices unless authorised under that Act or another law, including a law of the Commonwealth.[12] However, it also contains an application provision, stating that the Act does not apply to certain Commonwealth agents, including ASIO personnel, in the course of performing their agency's functions.[13]

19. Queensland, Tasmania and the ACT do not have a general prohibition on the use of tracking devices subject to specified exceptions, such as where the use is authorised under an Australian law. These jurisdictions have only enacted a specific prohibition on certain uses of listening devices by all persons (including the Crown) subject to specified exceptions including authorisation under another law.[14] They also have separate statutory authorisation regimes for their law enforcement agencies to use surveillance devices, but this legislation does not apply to ASIO.[15]

20. Consequently, in these jurisdictions – provided that there was no offence or tort involved – ASIO would not be subject to even the minimal statutory requirements proposed in Schedule 2 to the Bill, to use a tracking device in a public place. For example, the prescribed authorisation threshold[16] and requirement to make a request to a designated 'authorising officer' of a particular level of seniority[17] would

[12] *Surveillance Devices Act 1999* (Vic), section 8.
[13] Ibid, paragraph 5(b).
[14] *Invasion of Privacy Act 1971* (Qld), section 43; *Listening Devices Act 1991* (Tas), section 5; and *Listening Devices Act 1992* (ACT), section 4.
[15] *Police Powers and Responsibilities Act 2000* (Qld) (Chapter 13); *Police Powers (Surveillance Devices) Act 2006* (Tas); and *Crimes (Surveillance Devices) Act 2010* (ACT).
[16] Bill, Schedule 2, item 8, inserting proposed subsection 26G(6) of the ASIO Act.
[17] Ibid, inserting the definition of 'authorised officer' in section 22 of the ASIO Act, and proposed section 26G.

not apply. There would be no statutory maximum duration for the use of a tracking device,[18] or statutory reporting[19] and record-keeping[20] obligations.

21. Rather, the imposition of any equivalent limitations or restrictions to those in the Bill would be solely at the discretion of ASIO (in setting internal policies) or the Minister for Home Affairs (in amending the ASIO Guidelines issued under section 8A). The sole basis for the different sources of legal obligation, and any differences in applicable standards, would be the geographical location of the operation.

Law Council concerns

Arbitrariness

Differences in authorisation requirements based on a target's physical location

22. The Law Council is concerned that proposed subsection 33(4) of the ASIO Act would create arbitrary differences in ASIO's obligations to obtain a statutory internal authorisation, depending on the State or Territory in which the target is located when the device is installed and used at a particular point in time.

23. Consequently, it would largely be individual State and Territory Parliaments – not the Australian Parliament – that control whether ASIO is required to obtain a statutory internal authorisation to install, use, maintain or recover a tracking device in their respective jurisdictions. It is conceivable that State and Territory Parliaments may not have ASIO in their specific contemplation when they are enacting or amending their surveillance legislation of general application in their jurisdictions.

Inconsistency with the requirements of the *Intelligence Services Act 2001* (Cth)

24. Further, proposed subsection 33(4) of the ASIO Act would be inconsistent with the authorisation requirements applying to the Australian intelligence agencies governed by the ISA. These are the Australian Secret Intelligence Service (**ASIS**), the Australian Signals Directorate (**ASD**) and the Australian Geospatial-Intelligence Organisation (**AGO**).

Authorisation requirements

25. Sections 8 and 9 of the ISA require ASIS, ASD and AGO to obtain a ministerial authorisation to produce intelligence on an Australian person who is outside Australia, which includes the use of a tracking device.[21] The requirement for these agencies to obtain a ministerial authorisation **does not** depend on whether the conduct involved in producing the intelligence is unlawful under Australian law.[22] There is also no ability for these agencies to dispense with the ministerial

[18] Ibid, inserting proposed paragraph 26H(3)(b) of the ASIO Act.
[19] Ibid, Schedule 2, item 16, inserting proposed section 34AAB of the ASIO Act; and item 21, inserting proposed subsection 94(2BD) of the ASIO Act.
[20] Ibid, Schedule 2, item 8, inserting proposed section 26Q of the ASIO Act.
[21] See especially: ISA, paragraph 8(1)(a)(i) (Ministers must issue directions to their agencies to obtain a Ministerial authorisation to undertake any activity or series of activities for the specific purpose of producing intelligence on an Australia person, or activities which include the specific purpose of producing intelligence on an Australian person). Section 9 sets out the criteria the Minister must apply to grant an authorisation.
[22] Rather, there is a statutory immunity from criminal and civil liability under section 14 of the ISA in respect of any act that is undertaken by an agency official in the proper performance by that agency of its functions. Under subsections 14(2B) and (2C), the IGIS can issue a prima facie evidentiary certificate as to whether an act was undertaken in the 'proper performance' of an agency's functions.

authorisation requirement merely because no Australian law would prohibit a private individual or body corporate from carrying out the same activity.

26. The Law Council considers that the approach in the ISA to the design of authorisation requirements appropriately reflects the unique status of an intelligence agency, as distinct to a private person. The requirements in the ISA clearly reflect the unique and intrusive functions of an intelligence agency, the status of such an agency as an emanation of the State, its resourcing and technical capability, and its capacity to make subsequent use of intelligence.

Authorisation criteria

27. It is also worth noting that the criteria in section 9 of the ISA for the granting of ministerial authorisations to use tracking devices on Australian persons are considerably higher than the criteria proposed in the Bill for the issuing of statutory internal authorisations.

28. Under section 9 of the ISA, the agency's Minister must be satisfied that any activities done in reliance on the authorisation will be necessary for the proper performance a function of ASIS, ASD or AGO (as applicable). The Minister must also be satisfied that there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary, and that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to their purpose.

29. In contrast, the Bill merely requires the authorising officer in ASIO to be satisfied, on reasonable grounds, that using a tracking device will, or is likely to, substantially assist in the collection of intelligence in respect of a matter that is important in relation to security (as defined in section 4 of the ASIO Act).[23]

30. The statutory thresholds of necessity and proportionality in section 9 of the ISA better reflect the intrusions on personal privacy arising from the use of a tracking device (irrespective of the circumstances in which it is installed). As noted in the Law Council's original submission to the Committee, statutory issuing criteria directed to necessity and proportionality are a far stronger safeguard than an administrative requirement in ASIO's Guidelines.

Inconsistent thresholds and accountability requirements

31. Further, as noted above, if ASIO was not required to obtain a statutory internal authorisation to use a tracking device in a particular State or Territory, its use of that device would not be subject to the statutory authorisation thresholds and other transparency and accountability mechanisms proposed in the Bill. These include Ministerial reporting requirements on individual statutory internal authorisations,[24] annual reporting,[25] and obligations to keep written records of each statutory internal authorisation on a central register.[26]

32. If the Bill is passed in its present form, ASIO's reporting and record-keeping obligations in relation to its use of statutory internal authorisations would not provide the Attorney-General with a complete and therefore accurate picture of ASIO's warrantless use of tracking devices. Similarly, the other Ministers and

[23] Bill, Schedule 2, item 8, inserting proposed subsection 26G(6) of the ASIO Act.
[24] Ibid, Schedule 2, item 17, inserting proposed section 34AAB of the ASIO Act.
[25] Ibid, Schedule 2, item 21, inserting proposed subsection 94(2BD) of the ASIO Act.
[26] Ibid, Schedule 2, item 8, inserting proposed section 26Q of the ASIO Act.

Parliamentarians to whom ASIO's classified annual report must or may be given – including members of the Committee – will also not be able to obtain the full picture of ASIO's warrantless use of tracking devices from that report.[27]

Legal risk and uncertainty

Cross-border movement of targets

33. The operation of proposed subsection 33(4) could also create significant complexity, uncertainty and legal risk if a target were to cross State or Territory borders, given the substantial variation in State and Territory surveillance device legislation.

34. For example, ASIO may decide not to obtain a statutory internal authorisation to use a tracking device on a person who is in Victoria, in reliance on proposed subsection 33(4) and the exemption of ASIO from the general prohibition in the *Surveillance Devices Act 1999* (Vic). However, if that person moved from Victoria into New South Wales, the continued use of the device in New South Wales would require a statutory internal authorisation because of the prohibition in the *Surveillance Devices Act 2007* (NSW).

35. It is readily conceivable that individuals being targeted by an ASIO surveillance operation may move quickly between multiple jurisdictional borders, including in circumstances which may be unforeseen by ASIO. This would create a high risk of ASIO using the tracking device unlawfully. The Law Council submits that the Bill should remove the legal compliance risk to ASIO arising from differences in State and Territory surveillance legislation when a target moves across jurisdictions. The Bill should include a provision requiring ASIO to obtain a statutory internal authorisation to use a tracking device, in all circumstances in which it is not required to obtain a surveillance device warrant.

36. Further complexity, uncertainty and potential arbitrariness may arise if an intelligence operation targeted a body corporate or body politic, whose individual officers were disbursed across multiple States and Territories (such as staff or office holders of a body corporate, or diplomats or visiting foreign officials of a body politic). In these circumstances, the location of the individuals in a particular State or Territory would determine whether ASIO required a statutory internal authorisation.

37. Compliance with legal authorisation requirements in such operations may be particularly complex and high-risk, as larger numbers of individuals will conceivably be moving between multiple jurisdictions. It may also produce arbitrariness in that there will be variation in the applicable authorisation requirements for individuals who are working for the same body corporate or body politic being targeted, based solely on the geographical location of each individual.

38. These compliance risks could lead to ASIO adopting a policy of routinely obtaining a statutory internal authorisation to use a tracking device in all States and Territories, despite not being required to in some of those jurisdictions because of proposed subsection 33(4). While the Law Council would be supportive of this practice, it would mean that proposed subsection 33(4) would not perform any useful function in relation to internal authorisations. This casts doubt on its necessity.

---

[27] For example, under section 46 of the *Public Governance, Performance and Accountability Act 2013* (Cth), ASIO must give the Minister for Home Affairs a copy of its classified annual report. Subsection 94(3) of the ASIO Act provides that a copy of the classified annual report must be given to the Opposition Leader. The PJCIS may also access ASIO's classified annual report in the performance of its functions to review ASIO's administration and expenditure under paragraph 29(1)(a) of the ISA.

39. Further, the legal profession and the wider public would derive far greater assurance if any such policy were given legal effect in the Bill, as an explicit statutory obligation on ASIO to obtain an authorisation under proposed section 26G. An internal policy of ASIO is vulnerable to unilateral change or repeal by ASIO itself, and in any event is likely to be withheld from the public due to its classified nature. A statutory approval obligation, which is a condition of exercising an intrusive surveillance power, would provide a substantive legal safeguard against misuse of that power. Mere administrative obligations, such as requirements in policy or the ASIO Guidelines set by the Minister for Home Affairs, are not a legal safeguard.

Common law of tort

40. Further, when ASIO is operating in a State or Territory whose surveillance device legislation does not contain a general prohibition on the use of tracking devices,[28] it will be necessary to consider the law of tort. ASIO could rely on proposed subsection 33(4) not to obtain a statutory internal authorisation if the conduct involved in installing and using a tracking device in a public place or on the exterior of a vehicle did not constitute a tort, such as trespass to chattels or assault.

41. However, determining whether a particular installation and use of a tracking device may amount to a common law tort will involve a highly fact-specific assessment of the actions involved in installing and using the tracking device. It may not be possible to know exactly how a device will be installed in a public place until the time of its installation, as there will be many uncontrollable variables which may change rapidly. Consequently, it may be impossible (and potentially improper) for ASIO lawyers to give definitive advice to operational personnel, before an operation commences, that a statutory internal authorisation is not required.

42. This would leave a potentially complex legal issue – namely, determining the application of the common law of tort – to the judgment of individual intelligence officers during a surveillance operation (including decision-making about whether it is practicable to seek immediate legal advice). In addition to creating a significant compliance risk for ASIO, this could place individual ASIO officers in the invidious position of having to bear that risk for their agency.

43. As with the above comments on the cross-border movement of targets, it may be that ASIO chooses to manage these compliance risks by adopting a policy of routinely obtaining a statutory internal authorisation to use a tracking device in all States and Territories. However, if this is the intended means of managing legal risk, it would suggest that proposed subsection 33(4) is unnecessary in relation to tracking devices. A statutory obligation on ASIO to obtain an internal authorisation under proposed section 26G would provide a far more rigorous check and balance on its power to exercise a highly intrusive surveillance power without a warrant.

Amendments to proposed subsection 33(4) of the ASIO Act

44. If the Committee supports the enactment of the proposed internal authorisation framework for the use of tracking devices, the Law Council recommends that the Bill should be amended to require ASIO to utilise one of three sources of statutory authority in **all cases**. Namely, ASIO must obtain a surveillance device warrant or a statutory internal authorisation, or consent-based warrantless use (as applicable).

[28] As noted above, these jurisdictions are currently Victoria, Queensland, Tasmania and the ACT.

45. This approach would facilitate clarity and certainty. It would remove practical complexities and potential arbitrariness arising from differences in individual State and Territory laws, and the cross-border movement of targets. It would also ensure that there is no ability for ASIO to effectively bypass the statutory internal authorisation framework, based on the contents of State or Territory legislation as in force from time-to-time, without the Australian Parliament having visibility or control.

46. While the submission of the Inspector-General of Intelligence and Security (**IGIS**) to the present inquiry has noted an expectation about how ASIO will practically operate under proposed subsection 33(4) to manage legal risks of the kind outlined above,[29] the Law Council considers that the policy underlying the provision is fundamentally defective. This cannot be cured through retrospective oversight of ASIO's activities in reliance on that provision, or by the exercise of discretion by ASIO in making classified operational policies, or the Minister in amending the ASIO Guidelines.

47. Rather, the Bill should not include a provision that would make it lawful for ASIO to use a tracking device without any form of statutory approval in some jurisdictions, and would create a significant compliance risk. If proposed subsection 33(4) is enacted, the public will not have a reasonable basis on which to be assured that an intrusive surveillance power is subject to adequate legal safeguards, in the form of statutory approval requirements, to prevent both deliberate and inadvertent misuse.

48. As the (then) UK Independent Reviewer of Terrorism Laws, David Anderson QC, wrote in 2015, 'respected independent regulators [or oversight bodies] continue to play a vital and distinguished role. But in an age where trust depends on verification, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency'.[30] The Law Council considers that the Bill, as introduced, lacks these crucial elements for building and maintaining public trust in any warrantless exercise of intrusive surveillance powers. The following recommendation would go some way towards integrating those elements.

Recommendation – statutory authorisation requirements for tracking devices

- **If the Committee supports the enactment of the internal authorisation framework, then Schedule 2 to the Bill should be amended to prohibit ASIO from using a tracking device without authorisation under one of the following statutory heads of power (as applicable):**
  - **a surveillance device warrant under existing s 26 (if the conduct involved in installing, using, maintaining or recovering the device would involve an offence, or is otherwise excluded from an internal authorisation by proposed s 26K); or**
  - **an internal authorisation under proposed s 26G (if the tracking device is to be installed in a public place, including on the exterior of a vehicle in a public place, and does not exceed the limits of authority under proposed ss 26J and 26K); or**
  - **section 26E (if the other person consents to the installation, use, maintenance and recovery of the tracking device).**

[29] IGIS, *Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the ASIO Amendment Bill*, (July 2020), 25. The IGIS emphasised record-keeping of ASIO's internal decision-making.
[30] David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), 246.