Australian Government
Office of the Australian Information Commissioner

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 – Submission to the Parliamentary Joint Committee on Intelligence and Security

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
1 March 2021

OAIC

Contents

1. Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (Committee) on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Bill).[1]

2. The Bill seeks to amend the *Surveillance Devices Act 2004* (Cth) (Surveillance Devices Act), the *Crimes Act 1914* (Crimes Act), and associated legislation, to introduce three types of warrants that would be available to the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC)[2] for the purposes of investigating and disrupting serious online crime. These warrants are:

   - data disruption warrants (DDWs) which enable the AFP and the ACIC to modify, add, copy, or delete data for the purposes of frustrating the commission of serious offences online
   - network activity warrants (NAWs), which permit access to devices and networks used by suspected criminal networks for intelligence gathering purposes
   - account takeover warrants (ATWs), which provide the AFP and the ACIC with the ability to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation.

3. The Australian privacy framework recognises that the right to privacy needs to be balanced with public interest considerations but where it is curtailed, privacy impacts must be reasonable, necessary, and proportionate for the achievement of the particular policy objective.

4. The OAIC acknowledges the importance of law enforcement agencies being authorised to respond to cyber-enabled and serious crime. However, the Bill's proposed powers are wide-ranging and coercive in nature. For example, DDWs and NAWs may authorise entering specified premises, removing computers or data, and intercepting communications.[3] NAWs can authorise the use of surveillance devices,[4] and both DDWs and NAWs may authorise the concealment of certain activities done under these warrants.[5]

5. These powers may adversely impact the privacy of a large number of individuals, including individuals not suspected of involvement in criminal activity, and must therefore be subject to a careful and critical assessment of their necessity, reasonableness and proportionality. Further, given the privacy impact of these law enforcement powers on a broad range of individuals and networks, they should be accompanied by appropriate privacy safeguards.

6. The OAIC considers that the Bill requires further consideration to better ensure that any adverse effects on the privacy of individuals which result from these coercive powers are

[1] https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6623_first-reps/toc_pdf/20144b01.pdf;fileType=application%2Fpdf
[2] The ACIC, formerly known as the Australian Crime Commission (ACC), was established under the *Australian Crime Commission Act 2002* (Cth) and was formed when the ACC and CrimTrac merged in 2016.
[3] Bill, Sch1 s 27KE & 27KP.
[4] Bill, Sch1 s 27KP.
[5] Bill, Sch1 s 27KE & 27KP.

minimised, and that additional privacy protections are included in the primary legislation.

2. About the OAIC and the *Privacy Act 1988* (Cth)

7. The OAIC has regulatory oversight of the *Privacy Act 1988* Cth (Privacy Act), which sets out how Australian Privacy Principle (APP) entities (including most Australian Government agencies, and all private sector and not-for-profit organisations with an annual turnover of more than $3 million) must collect, use and disclose individuals' personal information.[6]

8. The Privacy Act includes provisions which recognise the unique nature of intelligence and enforcement bodies. For example, the ACIC is exempt from the operation of the Privacy Act,[7] and the AFP is an 'enforcement body',[8] meaning it can rely on exceptions from certain personal information management requirements in particular circumstances. Accordingly the importance of including appropriate safeguards in legislation that enables the coercive or covert collection of a broad range of personal information, including from individuals not suspected of involvement in criminal activities, commensurately increases.

9. Under section 28A(2) of the Privacy Act the Australian Information Commissioner (Commissioner) has the function of examining a proposed enactment and minimising any adverse effects on the privacy of individuals.

3. Warrants

10. The Bill outlines the conditions under which an officer of the AFP or ACIC may apply for a warrant[9] and the factors that a Judge, Administrative Appeals Tribunal (AAT) member or a magistrate in the case of an ATW (issuing authority) must consider before issuing that warrant.[10]

11. The OAIC makes recommendations below regarding additional safeguards that should be included in the Bill to ensure that impacts on individuals' privacy are reasonable, necessary and proportionate, noting the nature and scope of personal information that could be accessed under these warrants.

Mandatory consideration of the impacts on privacy

12. When issuing an ATW, the Bill requires a magistrate to have regard to the extent to which the privacy of any person is likely to be affected.[11] The OAIC considers this to be a privacy protective measure that would help to ensure that ATWs are only issued in circumstances where it is reasonable, necessary, and proportionate to do so following consideration of the privacy impacts.

---

[6] Personal information is defined in section 6(1) as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information is recorded in a material form or not'.
[7] Privacy Act, s 7(1)(a)(iv).
[8] Privacy Act, s 6.
[9] For example, Bill, Sch 1 Item 13, ss 27KA & 27KB.
[10] See, for example, Bill Sch2 pt 1 Item 9 s 27KM(2) & Sch1 pt 1 Item 13 27KC(2).
[11] Bill, Sch3 Item 4 s 3ZZUP(2)(C).

13. However, this protection does not apply to DDWs and NAWs.[12] The OAIC considers that DDWs and NAWs have the comparable potential to impact the privacy of individuals, including third parties not the subject of the warrant, as ATWs. For example, DDWs and NAWs could empower law enforcement officers to collect a similar volume of personal information to an ATW. As noted by the Senate Standing Committee for the Scrutiny of Bills, 'it is unclear why privacy is a mandatory consideration in relation to account takeover warrants only and should not also apply to data disruption and network activity warrants.'[13]

14. The OAIC considers that it is appropriate that issuing authorities be required to consider the extent to which DDW and NAW warrants are likely to affect the privacy of individuals when determining an application for these warrants.

Recommendation 1 – The Bill be amended to require issuing authorities to consider the impact of the warrant on the privacy of any individual when determining applications for DDWs and NAWs, in addition to ATWs.

Duration

15. The Bill provides that each type of warrant may be issued for a period of no more than 90 days,[14] but that law enforcement officers may apply for 90-day warrant extensions without limit.[15] The OAIC considers that the ability to indefinitely renew warrants and the subsequent collection of personal information could amount to ongoing surveillance and a significant privacy intrusion, not only in respect of the subject or subjects of the warrant but also potentially a large number of individuals incidentally connected to that subject.

16. The OAIC recommends that the Bill be amended to:

- limit the number of warrant extensions that can be sought in respect of the same or substantially similar circumstances
- require the issuing authority to consider the privacy impact on any individual arising from the extension of the warrant to ensure that the potential law enforcement benefits are necessary and proportionate to this impact.

[12] Bill, Sch1 Item 13 s 27KC & Sch2 pt 1 Item 9 s 27KM.
[13] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 1 of 2021, 29 January 2021) 31.
[14] Bill, Sch1 Item 13 s 27KD, Sch2 p1 Item 9, s 27KN & Sch3 Item 4, s 3ZZUQ.
[15] Bill, Sch1 Item 13 ss 27KF(1)(a) & (6), Sch2 pt 1 Item 9 s 27KQ(1)(a) & (6), Sch3 Item 4 s 3ZZUS(1)(a).

Recommendation 2 – The Bill be amended to:

- limit the number of warrant extensions that can be sought in respect of the same or substantially the same circumstances
- require the issuing authority to consider the privacy impact on any individual arising from the extension of the warrant to ensure that the potential law enforcement benefits are necessary and proportionate to this impact.

Judicial oversight

17. The OAIC has previously recommended judicial authorisation and oversight of the issuing of warrants.[16] However, the Bill also allows nominated AAT members to issue DDWs and NAWs who need not be judicial members.[17] When an adverse impact on privacy may be necessary, a commensurate increase in oversight, accountability, and transparency is required to strike an appropriate balance between any privacy impacts and law enforcement objectives.

18. Accordingly the OAIC recommends that the Bill be amended to only allow judicial authorisation of warrants under s 27KC and 27KM of the Bill.

Recommendation 3 – The Bill be amended to only allow for judicial oversight and authorisation of warrants issued under the Bill.

Reasonable grounds

19. The Bill allows a chief officer of the AFP or ACIC to apply for a warrant if that officer suspects that one or more 'relevant offences'[18] have been, are being, are about to be, or are likely to be committed. The officer must hold this suspicion (among others) on 'reasonable grounds'[19] to apply for the warrant. The issuing authority must then also be satisfied that there are 'reasonable grounds' for the suspicion.[20]

20. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. The High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person';[21] it 'involves an evaluation of the known facts, circumstances and

[16] See, for example, our previous submissions to the Independent National Security Legislation Monitor and to the Parliamentary Joint Committee on Intelligence and Security on the *Telecommunications and Other Legislation Amendment (Assistance And Access Act 2018.*
[17] Bill, Sch1, s 27KA(3) (for DDWs) & Sch2, s 27KK(3) (for NAWs).
[18] The Bill defines 'relevant offences' as 'a serious Commonwealth offence' or 'a serious State offence that has a federal aspect' (Sch3 Item 4 s 3ZZUK).
[19] Bill, Sch1 s 27KA(1) (for DDWs), Sch1, pt 1 Item 9 s 27KK(1) (for NAWs), & Sch3 Item 4 s 3ZZUN(1) (for ATWs).
[20] Bill, Sch1 s 27KC(1)(a) (for DDWs), Sch1, pt 1 Item 9 s 27KM(1)(a) (for NAWs), & Sch3 Item 4 s 3ZZUP(1) (for ATWs).
[21] *George v Rockett* (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ).

considerations which may bear rationally upon the issue in question'.[22] As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

21. Given the potential nature and scale of personal information that may be accessed through these warrants, the OAIC suggests that the Bill or Explanatory Memorandum (EM) be expanded to identify some of the objective circumstances that should be considered in determining whether there are 'reasonable grounds' to support the seeking and issuing of a warrant. Such criteria could assist in ensuring consistency in decision making.

Definition of 'criminal network of individuals'

22. The chief officer of the AFP or ACIC may apply for a NAW if that officer suspects on reasonable grounds that a group of individuals constitutes a 'criminal network of individuals.'[23] The Bill defines a criminal network of individuals as an 'electronically linked' group of two or more individuals, where one or more individuals in the group has:

- engaged, are engaging, or are likely to engage, in conduct that constitutes a relevant offence, or
- facilitated, are facilitating, or are likely to facilitate, the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence.[24]

23. The OAIC considers that this definition has the potential to include a significant number of individuals, including third parties not the subject or subjects of the warrant who are only incidentally connected to the subject or subjects of the warrant. The seriousness of this impact upon privacy requires further mitigation with commensurate safeguards. The OAIC recommends amending the Bill to narrow the definition of 'criminal network of individuals'.

Recommendation 4 – The Bill be amended to narrow the definition of a 'criminal network of individuals'.

Emergency authorisations

24. The Bill authorises law enforcement officers to use the powers conferred under DDWs and ATWs without first acquiring a warrant in prescribed emergency circumstances. In these circumstances, law enforcement officers can apply[25] to an 'appropriate authorised officer',[26] in place of an issuing authority. The appropriate authorised officer must, within 48 hours after giving an emergency authorisation, apply to a magistrate for retrospective approval of that authorisation.[27]

---

[22] *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).
[23] Bill, Sch2 Item 9 s 27KK(1)(a).
[24] Bill, Sch2 pt 1 Item 8 s 7A(1).
[25] Bill, Sch1 Item 15 (proposed s 28(1C) of the *Surveillance Devices Act 2004* (Cth)) & Sch3 Item 4 s 3ZZUX.
[26] Defined in s 6A of the *Surveillance Devices Act 2004* (Cth) and proposed s 3ZZUM of the *Crimes Act 1914* (Cth). The definition includes the head or deputy head of the agency, and certain executive level officers.
[27] Bill, Sch3 Item 4 s 3ZZVA(1).

25. The OAIC considers that other more appropriate mechanisms to seek a warrant in these kinds of emergency circumstances should be considered. For example, other sections of the Bill would allow applications for warrants to be made by telephone, fax, email, or any other means of communication.[28] The Senate Standing Committee for the Scrutiny of Bills raised similar concerns, and found that this power 'has the potential to unduly trespass on the right to privacy.'[29] The Senate Standing Committee considered that, while they would expect explanatory materials to provide a detailed justification for such provisions, the statement of compatibility provided 'no such justification'.

26. The OAIC recommends that the Bill be amended to include additional privacy safeguards for the access of personal information in emergency circumstances, for example with reference to alternative application mechanisms. This would, in our view, achieve a more appropriate balance between any privacy impacts and law enforcement objectives.

Recommendation 5 – The Committee consider amendments to exclude warrant approval by an 'appropriate authorised officer' and consider alternative external warrant approval mechanisms, such as applications made by telephone, fax, email, or any other means of communication, in emergency situations.

4. Prohibited uses of information

27. The Bill allows any information obtained through an emergency authorisation to be 'dealt with in a manner specified in the order, so long as the manner does not involve the destruction of that information'.[30] This requirement applies even in instances where the issuing agency does not approve the 'appropriate authorised officer's' emergency authorisation.

28. The EM states that this information, 'while improperly obtained', may still 'be required for a permitted purpose, such as an investigation'.[31] The OAIC notes that the prohibition on the destruction of this information could have significant adverse impacts on the privacy of individuals, as law enforcement agencies would be required to retain information despite an issuing authority subsequently denying a warrant for its collection. The OAIC is unclear of the rationale for retention in such circumstances and therefore considers that information that is later deemed to have been improperly obtained should be quarantined and destroyed expeditiously.

Recommendation 6 – The Bill be amended to require that law enforcement agencies destroy any information collected under an emergency authorisation that was subsequently denied.

[28] Bill, Sch1 Item 13 ss 27KB & 27KL & s Sch3 Item 4 s 3ZZUN(2)(b).
[29] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 1 of 2021, 29 January 2021) 29-48.
[30] Bill, Sch3 Item 4 s 3ZZVC(4) & Sch1 Item 23 s 35B(4).
[31] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 1 of 2021, 29 January 2021) 35.

29. The Bill provides that a chief officer of the AFP or the ACIC must cause protected information[32] or protected network activity warrant information[33] to be destroyed either as soon as practicable or within a period of 5 years.

30. Noting the potential volume and sensitivity of information collected under each warrant, the OAIC recommends that the Bill include a mechanism that would require regular reviews of the ongoing utility of collected information. This would also help to ensure that collected information, including personal information, is deleted as soon as it is no longer required for the purposes for which it was collected.

31. As with any database containing personal information, the privacy and security risks to that information increases commensurately with the volume of information retained. The OAIC recommends that the Committee also consider whether the 5-year retention period is appropriate. The OAIC notes that this approach would be consistent with APP 11.2, which requires entities to take reasonable steps to destroy or de-identify the personal information that it no longer needs.

Recommendation 7 – The Bill be amended to impose a positive, regular requirement on collecting agencies to consider the utility of the collected information and take active steps to destroy it when it is no longer necessary for the purposes of criminal investigations.

5. Privacy Impact Assessments

32. The Bill introduces new personal information management practices, such as those relating to the transfer of complaints between certain integrity bodies.[34] The OAIC recommends that a Privacy Impact Assessment (PIA) be conducted by these bodies as well as other entities affected by these new personal information handling arrangements.

33. A PIA is a systematic written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. Undertaking PIAs is a key component of a 'privacy by design' approach. They can also help to build the community's trust that privacy risks have been identified, and protections embedded, at the design stage of a new project involving personal information handling.

34. The *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Privacy Code) requires Australian Government agencies subject to the Privacy Act to conduct a PIA for all 'high privacy risk projects'. A project may be a high privacy risk project if the agency reasonably considers that the project involves new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

35. We also note that PIAs should be revisited and updated when changes to a project are considered, and, in some instances, it may be necessary to undertake another PIA. The OAIC

[32] Bill, Sch3 Item 4 s 3ZZVJ & *Surveillance Devices Act 2004* (Cth), s 46(b).
[33] Bill, Sch2 pt 1 Item 20 s 46AA(1)(ii).
[34] See, for example, Bill, Sch2, pt2 Items 68, 91-92 - 11(4A), 32(AD).

has published a *Guide to undertaking privacy impact assessments* and *When do agencies need to conduct a privacy impact assessment?* to assist agencies in meeting their Privacy Code obligations.

36. Thank you for the opportunity to provide a submission to the Committee. The OAIC is available to provide further information or assistance as required.