COMMONWEALTH OMBUDSMAN

Submission by the Commonwealth Ombudsman

Parliamentary Joint Committee on Intelligence and Security

Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Submission by the Commonwealth Ombudsman, Michael Manthorpe PSM

February 2021

Introduction and summary

1. On 8 December 2020, the Parliamentary Joint Committee on Intelligence and Security commenced a review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill).
2. This submission outlines the role of the Office of the Commonwealth Ombudsman (the Office), details the Office's existing oversight functions and considers the Bill and its impact on these oversight functions.

Our role

3. The purpose of the Office is to:
    - provide assurance that Australian government entities and prescribed private sector organisations, that the Office oversees, act with integrity and treat people fairly
    - influence enduring systemic improvement in public administration in Australia and the region.
4. We aim to achieve our purpose through the following objectives:
    - Influencing Australian and Australian Capital Territory government entities to improve public administration and complaint handling systems through public reports, recommendations and direct engagement.
    - Providing an efficient, effective and accessible government complaint handling service.
    - Undertaking oversight and assurance activities relating to the integrity of Australian government entities, Australian Capital Territory government entities and prescribed private sector organisations.
    - Providing effective and impartial industry complaint handling services and consumer information.
    - Delivering capacity-building programs under the Australian Aid arrangements to support ombudsmen and allied integrity bodies to improve governance and accountability.

Oversight and assurance

5. The Office conducts compliance inspections and reviews of 23 law enforcement, integrity and regulatory agencies' use of certain covert, intrusive and coercive powers. We engage with agencies, inspect relevant records and review agencies' policies and processes to assess their compliance with statutory requirements.
6. The covert nature of many of the powers we inspect means we are unlikely to receive complaints about their use, so our role in monitoring their use and reporting our findings is important in providing transparency to the Parliament and the public about whether agencies use their powers appropriately.
7. Currently, the Office oversees the following activities under Commonwealth legislation:
    - telecommunications interceptions under Chapter 2 of the *Telecommunications Interception and Access Act 1979* (the TIA Act)
    - preservation of and access to stored communications under Chapter 3 of the TIA Act
    - access to telecommunications data under Chapter 4 of the TIA Act
    - use of industry assistance powers under Part 15 of the *Telecommunications Act 1997*

- surveillance device and computer access warrant activity under the *Surveillance Devices Act 2004* (the SD Act)
- delayed notification search warrant activity under Part IAAA of the *Crimes Act 1914* (Crimes Act)
- monitoring of compliance with control orders under Part IAAB of the Crimes Act
- conduct of controlled operations under Part IAB of the Crimes Act
- coercive examinations conducted under the *Fair Work Act 2009* and the *Building and Construction Industry (Improving Productivity) Act 2016*.

The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 and its impact on our oversight functions

8. The Bill would introduce new powers into the SD Act and the Crimes Act for the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC), to combat serious crime online, specifically:
    - the data disruption warrant to enable the disruption of online criminal activity
    - the network activity warrant to enable intelligence collection relating to online criminal networks
    - the account takeover warrant to facilitate evidence gathering through taking control of an online account.
9. The Department of Home Affairs consulted the Office throughout the Bill's development and incorporated the majority of our feedback.

The interrelation between the Office and the IGIS

10. The Bill proposes extending the Office's oversight role within the Crimes Act to the account takeover warrant regime.
11. The Bill also seeks to extend the Office's oversight role within the SD Act to the data disruption warrant regime, while tasking the Inspector-General of Intelligence and Security (the IGIS) with oversight of the network activity warrant regime.
12. While introducing IGIS oversight of AFP and ACIC use of electronic surveillance would mark a convergence of our offices' stakeholder bases, the Office considers this proposal consistent with the broader delineation of our respective roles:

Comparison of IGIS and Ombudsman oversight of covert activity

	Ombudsman	**IGIS**
Purpose of covert activity	Criminal law enforcement	Intelligence collection
Assessment breadth	Legal compliance and administrative best practice	Legal compliance, propriety and consistency with human rights

13. The Office is satisfied that measures in the Bill to facilitate information sharing between the Office and the IGIS ensure efficacy in our respective functions, in line with recommendation 171.f of the 2019 *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (the Richardson Review).

Consistency of procedures with existing covert power frameworks

14. The Office recognises the challenge of navigating multiple principles, interests and policy objectives in developing new legislation, particularly where these factors are not immediately congruent.

15. In some instances, the Bill demonstrates a prioritisation of internal legislative consistency, rather than consistency between similar covert power types. It is our view that it may be more appropriate to align new covert powers more broadly with existing covert powers, particularly in regard to:

    - issuing officers for account takeover warrants
    - consideration of privacy impacts for data disruption warrants, and
    - requiring an affidavit in support of an account takeover warrant.

16. The Bill proposes to vest authority in magistrates to issue account takeover warrants, consistent with overt powers in the Crimes Act.[1] The Office suggests that eligible judges and nominated AAT members would be more appropriate issuing authorities, consistent with covert regimes for delayed notification search warrants (Crimes Act), surveillance device warrants and retrieval warrants (SD Act), computer access warrants (SD Act), telecommunication interception warrants (TIA Act), proposed data disruption warrants (the Bill), and proposed network activity warrants (the Bill).[2]

17. Further, the Bill does not require issuers to consider privacy impacts when determining whether to issue a data disruption warrant.[3] The Office acknowledges that it will not always be possible to determine the extent of privacy interference in using the data disruption power. However, it is our experience that this is also the case for other covert powers which nonetheless require a consideration of privacy impacts (or less intrusive alternatives) in determining applications. These include delayed notification search warrants (Crimes Act), surveillance device warrants and retrieval warrants (SD Act), computer access warrants (SD Act), telecommunication interception warrants (TIA Act), proposed account takeover warrants (the Bill), and proposed network activity warrants (the Bill).[4] Requiring issuers to consider privacy or less intrusive means of obtaining information or disrupting activity ensures that they have turned their mind specifically to the balance between the right to privacy and the safety of the Australian community when deciding whether to authorise the use of particular powers.

18. Additionally, the Bill requires account takeover warrant applications to provide 'sufficient information' to enable the magistrate to make a determination.[5] It is our view that the account takeover regime should require an affidavit setting out the grounds of an application, consistent with delayed notification search warrants (Crimes Act), surveillance device warrants and retrieval warrants (SD Act), computer access warrants (SD Act)

---

[1] Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 3 s 3ZZUP.
[2] *Crimes Act 1914* (Cth) s 3ZZAD, *Surveillance Devices Act 2004* (Cth) s 11, *Telecommunications (Interception and Access) Act 1979* (Cth) ss 46 and 46A, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 1 s 27KC and sch 2 s 27KM.
[3] Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 1 s 27KC.
[4] *Crimes Act 1914* (Cth) s 3ZZBD(2)(c), *Surveillance Devices Act 2004 (*Cth*)* ss 16(2)(c), 24(2)(a) and 27C(2)(c), *Telecommunications (Interception and Access) Act 1979* (Cth) ss 46(2)(a) and 46A(2)(a), Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 3 s 3ZZUP(2)(c) and sch 2 s 27KM(2)(e).
[5] Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 3 ss 3ZZUN(3) and 3ZZVA(2)(a).

telecommunication interception warrants (TIA Act), proposed data disruption warrants (the Bill), and proposed network activity warrants (the Bill).[6]

Proposed agency reporting obligations

19. In relation to the Bill's proposed reporting obligations, the Office notes there is no requirement for the AFP and the ACIC to report on the details of coercive assistance orders given in the course of executing data disruption and account takeover warrants, despite introducing this requirement for network activity warrants.[7]

20. Statutory reporting on covert and coercive powers creates transparency and accountability. Reports assist oversight agencies to conduct inspections and test record keeping consistency and accuracy.

21. Ultimately, reports enable public awareness of how covert powers are used and help to provide public assurance that they are used as intended. In our view, the details of assistance orders should be required to be reported across all applicable regimes.

Proposed inspection and reporting obligations of the Commonwealth Ombudsman

22. In relation to the data disruption warrant regime, the Bill proposes extending existing inspection and reporting requirements under the SD Act. While the Act requires six-monthly reporting on inspections conducted, it does not prescribe a minimum frequency of inspections of each agency subject to the Office's oversight.[8]

23. In relation to the account takeover warrant regime, the Bill imposes six-monthly inspection and six-monthly reporting obligations on the Office.[9] While this is consistent with the inspection and reporting requirements for the delayed notification search warrant regime, it does not align with the requirements for other Crimes Act regimes that we oversee.

24. The inspection and reporting requirements differ across the three Crimes Act regimes we oversee, namely delayed notification search warrants, monitoring of control orders and controlled operations.[10]

25. The Office suggests that the inspection and reporting requirements for the account takeover warrant regime may be more appropriately aligned with the 12-monthly inspection and reporting obligations of the controlled operations regime (Part IAB of the Crimes Act).[11] Aligning the account takeover oversight arrangements with the controlled operations framework better reflects the likely operational intersection between account takeover warrants and controlled operations, while providing the Office with more flexibility and discretion in managing our oversight functions and in line with recommendations 171.d and 171.e of the Richardson Review.

---

[6] *Crimes Act 1914* (Cth) s 3ZZBC(3), *Surveillance Devices Act 2004 (*Cth*)* ss 14(5)(b), 22(3) and 27A(8)(b), *Telecommunications (Interception and Access) Act 1979* (Cth) s 42, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 1 s 27KA(3)(b) and sch 2 s 27KK(4)(b).

[7] Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 1 s 49(2D)(d), sch 3 ss 3ZZVL and 3ZZVM sch 2 s 49(2E)(b)(xvi).

[8] *Surveillance Devices Act 2004* (Cth) ss 55(1) and 61(1).

[9] Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) sch 3 ss 3ZZVR(1) and 3ZZVX(1).

[10] *Crimes Act 1914* (Cth) ss 3ZZGB(1) and 3ZZGH(1), ss 3ZZUB(1) and 3ZZUH(1), ss 15HS(1) and 15HO(1).

[11] *Crimes Act 1914* (Cth) ss 15HS(1) and 15HO(1).