Chapter 1

Introduction and background

Introduction

1.1 On 28 November 2016, the Senate referred the following matter to the Committee of Privileges for inquiry and report:

(a) whether protocols for the execution of search warrants in the premises of members of Parliament, or where parliamentary privilege may be raised, sufficiently protect the capacity of members to carry out their functions without improper interference;

(b) the implications of the use of intrusive powers by law enforcement and intelligence agencies, including telecommunications interception, electronic surveillance and metadata domestic preservation notices, on the privileges and immunities of members of Parliament;

(c) whether current oversight and reporting regimes on the use of intrusive powers are adequate to protect the capacity of members of Parliament to carry out their functions, including whether the requirements of parliamentary privilege are sufficiently acknowledged;

(d) whether specific protocols should be developed on any or all of the following:

(i) access by law enforcement or intelligence agencies to information held by parliamentary departments, departments of state (or portfolio agencies) or private agencies in relation to members of Parliament or their staff,

(ii) access in accordance with the provisions of the *Telecommunications (Interception and Access) Act 1979* by law enforcement or intelligence agencies to metadata or other electronic material in relation to members of Parliament or their staff, held by carriers or carriage service providers, and

(iii) activities of intelligence agencies in relation to members of Parliament or their staff (with reference to the agreement between the Speaker of the New Zealand House of Representatives and the New Zealand Security Intelligence Service); and

(e) any related matters, including competing public interest considerations.

1.2 Although the initial terms of reference were proposed without consultation with this committee, they were amended prior to adoption, in accordance with its advice. The committee's advice was informed by the inquiry it was undertaking at the time of referral – the assessment of claims of parliamentary privilege made over documents seized under search warrant from both a senator's office and the home of a staff member, together with a possible contempt (the improper interference that had

arisen in the context of the execution of the search warrant). The committee reported on these matters in its 163rd and 164th reports.

1.3 In its 164th Report, the committee concluded that:

> … if it is to meet its stated purpose, the [National Guideline] must be revised to ensure that all persons involved in the execution of warrants understand and respect the requirement to quarantine information while claims of privilege are determined. This is a matter the committee will consider in its inquiry on the adequacy of parliamentary powers in the face of intrusive powers.[1]

1.4 In the limited statements made on the referral, the sponsoring senator indicated his view that the inquiry was about 'metadata domestic preservation orders and the chilling effect that such orders can have on the provision of information to members of parliament in order to enable them to carry out their functions.'[2]

1.5 At the beginning of the inquiry the committee agreed to publish a background paper which sets out the focus of the inquiry – ' … how the use of intrusive powers relates specifically to the operation and integrity of parliamentary privilege.'[3]

Background

Intrusive powers of concern in this inquiry

1.6 The term 'intrusive powers' lacks a precise definition, and there are a range of powers available to law enforcement and intelligence agencies that could be defined as such. For the purposes of this inquiry, however, the committee is particularly interested in issues of parliamentary privilege as they relate to powers to:

- enter and search premises and seize evidential material under search warrant;
- intercept live communications and conduct other electronic surveillance;
- access stored communications; and
- access telecommunications data ('metadata').

1.7 With the exception of access to telecommunications data, these powers are generally exercised on the basis of a warrant. Access to telecommunications data, which is provided for under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), generally does not require a warrant.[4]

1.8 The committee has given some consideration to the framework for the execution of search warrants in its 163rd and 164th reports. The legislative framework

---

1 Committee of Privileges, *Search warrants and the Senate*, 164th Report, March 2017, p. 19.

2 Hansard, 28 November 2016 pp. 3385-6.

3 Background paper agreed at meeting on 9 February 2017, and published on the committee's website, p. 1.

4 As explained below, access to a journalist's telecommunications data for the purposes of identifying a source does require a warrant.

for interception and access to telecommunications and telecommunications data is set out below.

Interception of communications – legislative framework

1.9 The TIA Act provides for enforcement agencies to apply for a warrant to intercept communications. Applications can be made in relation to a 'serious offence', which is defined in section 5D of the TIA Act.[5] While a range of interception warrant types are available, applications must satisfy the Issuing Officer as to the detailed requirements set out in section 46 the Act. In Victoria and Queensland, the Issuing Officer must also have regard to submissions made by a Public Interest Monitor.

1.10 The *Surveillance Devices Act 2004* (SD Act) governs the use of surveillance devices by agencies, including state and territory law enforcement agencies when they are using surveillance devices under Commonwealth laws.

1.11 The SD Act covers:

- data surveillance devices—devices or programs used on computers;
- listening devices—devices used to listen to or record conversations;
- optical surveillance devices—devices used to record visuals or observe activities; and
- tracking devices—devices used to locate or track a person or object.

1.12 The SD Act does not contain any prohibitions on the use of surveillance devices. The laws of the Australian states and territories generally contain prohibitions on surveillance devices, with exceptions for the investigation of state and territory offences. The Act complements the surveillance devices laws of the states and territories by allowing law enforcement agencies to obtain surveillance device warrants to help investigate federal offences and state offences with a federal aspect.

5 Section 5D sets out offences that are classified as 'serious offences', including murder, kidnapping, major federal drug offences, acts of terrorism, serious fraud and offences punishable by a maximum period of imprisonment of at least 7 years.

Access to stored communications content

1.13 The TIA Act also authorises criminal law enforcement agencies, including the AFP, to access stored communications content after obtaining a warrant from a court or tribunal.[6] A stored communication is defined in section 5(1) of the TIA Act as meaning a communication that:

(a) is not passing over a telecommunications system;

(b) is held on equipment that is operated by, and is in the possession of, a carrier; and

(c) cannot be accessed on that equipment, by a person who is not a party to the communications, without the assistance of an employee of the carrier.

1.14 Examples of stored communications include voicemails, emails, SMS and MMS messages held by a carrier. Importantly, access to stored communications provides access to the content of the communication[7] (whereas access to telecommunications data does not include access to communications content of the substance of a person's communications with others).

1.15 Warrants to access stored communications may be issued only in relation to a 'serious contravention', as defined in section 5E of the TIA Act.[8] In considering an application for a warrant, the Issuing Officer must have regard to requirements set out in section 116 of the TIA Act; these requirements mirror those in relation to warrants to intercept communications, as discussed above.

1.16 The TIA Act also provides a system for preserving certain stored communications that are held by a carrier, and thereby preventing the communications from being destroyed before they can be accessed under warrant. This system enables criminal law-enforcement agencies to give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specific in the notice. In relation to domestic

6 Members of a police force can also access communications without a warrant in certain emergency situations. As set out in Part 2-3 of the TIA Act, an emergency would involve a situation where a person is dying, is or has been seriously injured, or is likely to die or be seriously injured, and the interception is undertaken for the purposes of tracing the location of a caller.

7 Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 27 February 2015, p. 187.

8 The threshold for a 'serious contravention' is lower than for a 'serious offence'. For example, 'serious contraventions' include offences punishable by a maximum period of imprisonment of at least 3 years, and punishable by maximum fines of at least 180 penalty units for an individual.

preservation notices,[9] which cover stored communications that might relate to a contravention of certain Australian laws, there are two types of notice: historic domestic preservation notices, which cover stored communications that already exist and are held by the carrier on a particular day; and ongoing domestic preservation notices, which cover stored communications held by the carrier in a particular 30-day period. Preservation notices do not provide access to communications, which generally still requires a warrant.

1.17 The TIA also contains separate provisions authorising ASIO to engage in warranted interceptions and access to stored communications, and issue preservation notices, for the purpose of that organisation performing its statutory intelligence collection functions.

1.18 The SD Act authorises law enforcement agencies to use certain types of surveillance devices.[10]

Access to telecommunications data ('metadata')

1.19 The TIA Act permits Australian agencies to access telecommunications data—that is, data associated with a communication, such as telephone call records or account-holder names. Telecommunications data is colloquially referred to as 'metadata'. On its website, the Attorney-General's Department suggests that this data 'does not include the content or substance of a communication'.[11]

1.20 Access to telecommunications data does not require a warrant, unless (as explained below) the data of a journalist is sought for the purposes of identifying sources. Certain authorised officers in agencies may request that industry providers provide this data as part of investigations into crime, revenue and national security matters.

1.21 Officers may only request access to data after satisfying legal tests set out in the Act. Requests for access to data are subject to independent oversight by the Commonwealth Ombudsman, or by the Inspector-General of Intelligence and Security in the case of ASIO.

Journalist Information Warrant regime

1.22 The TIA Act prohibits agencies from authorising the disclosure of journalists' or their employers' telecommunications data—that is, their 'metadata'—for the

---

9 The AFP can also issue foreign preservation notices, which cover stored communications that might relate to a contravention of certain foreign laws. The AFP alone has this power, and can only issue a foreign preservation notice if a foreign country has made a request for the preservation in according with section 107P of the TIA Act.

10 The *Surveillance Devices Act 2004* complements state and territory surveillance legislation.

11 Attorney-General's Department, 'Overview of legislation', https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Overviewoflegislation.aspx.

purposes of identifying a source of the journalist without a warrant issued from an independent issuing authority.[12]

1.23 The TIA Act requires that, in considering an application for a journalist information warrant, the issuing authority (in the case of law enforcement agencies) or the Minister (in the case of ASIO) be satisfied that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the source.[13] In making that assessment, the issuing authority or Minister is required to have regard to the submissions made by a Public Interest Advocate evaluating the warrant application. Public Interest Advocates are senior members of the legal profession appointed by the Prime Minister for this purpose.[14]

1.24 There is no requirement that Public Interest Advocates be publicly identified. Equally, there is nothing to prevent the government from identifying a Public Interest Advocate, but to date it has refrained from doing so.

Oversight and accountability mechanisms

1.25 The TIA Act includes a number of oversight and accountability mechanisms. In particular, the Commonwealth Ombudsman has the power to inspect the records of enforcement agencies to ensure compliance with the Act, and the Inspector-General of Intelligence and Security has oversight of access to data by ASIO.[15] In addition, the Parliamentary Joint Committee on Intelligence and Security must be notified as soon as practicable of the issuing of any journalist information warrant, and has the opportunity to request briefings from the Commonwealth Ombudsman or the Inspector-General on any reports produced in relation to those warrants or authorisations.[16]

1.26 The TIA Act requires that enforcement agencies provide the Minister with an annual report indicating the number of data disclosure authorisations made under journalist information warrants and the number of journalist information warrants issued to the agency in that year. The Minister is in turn required to table an annual report in Parliament that includes this information.[17] The *Telecommunications (Interceptions and Access) Act 1979: Annual Report 2015–16*, was tabled on 14 August 2017; it reported that for the period between 13 October 2015 and

12 *Telecommunications (Interception and Access) Act 1979*, ss. 180G(1) and ss. 180H(1).

13 *Telecommunications (Interception and Access) Act 1979*, para. 180L(2)(b) and para. 180T(2)(b).

14 *Telecommunications (Interception and Access) Act 1979*, subpara. 180L(2)(v) and subpara. 180T(2)(b)(v).

15 Supplementary Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, pp. 47–48.

16 *Telecommunications (Interception and Access) Act 1979*, s. 185D.

17 *Telecommunications (Interception and Access) Act* 1979, para. 186(1)(i) and (j), and ss. 186(2) and (3).

30 June 2016, 33 authorisations were made under two journalist information warrants issued to the WA Police.[18]

1.27 ASIO is also required to include the number of journalist information warrants and authorisations made under such warrants in its classified annual report,[19] which is given to the Minister but the information may be deleted from the version of the report tabled in Parliament.

Existing protocols and guidance in relation to the exercise of intrusive powers where issues of parliamentary privilege may be raised

1.28 Of the abovementioned intrusive powers, only the exercise of search warrants is covered by an established protocol based on an agreement between the Parliament (through the Presiding Officers) and the executive. Specifically, a 2005 Memorandum of Understanding (MoU) between the presiding officers, the Attorney-General and the Minister for Justice and Customs records the process to be followed where the AFP proposes to execute a search warrant on premises occupied or used by a member of the Federal Parliament ('a Member'), including the Parliament House office of a Member, the electorate office of a Member, and the residence of a Member. The process agreed in the MoU is spelt out in the AFP's *National Guideline for the Execution of Search Warrants where Parliamentary Privilege may be involved* ('National Guideline').[20]

1.29 The AFP has also issued a *National Guideline on politically sensitive investigations*,[21] which includes some consideration of the interface between the AFP's investigative powers and parliamentary privilege. The guideline states that when issues of parliamentary privilege are likely to be encountered during an investigation, the functional management team should be consulted in the first instance. The relevant National Manager must also be consulted prior to conducting interviews with Members or executing search warrants upon a Member's premises. With regard to the execution of search warrants, the guideline also refers to the *National Guideline for the Execution of Search Warrants where Parliamentary Privilege may be involved*. Finally, the guideline suggests that when dealing with parliamentary privilege issues, AFP officers should also consider consulting with AFP

---

18 Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979: Annual Report 2015–16*, p. 58.

19 *Australian Security Intelligence Organisation Act 1979*, para. 94(2A)(h) and (i).

20 For a copy of the National Guideline, and the MoU from which it is derived, see http://www.aph.gov.au/~/media/02%20Parliamentary%20Business/22%20Chamber%20Documents/Dynamic%20Red%20-%2045th%20Parliament/01%20-%2030%20August%202016/SSG025P1016083017291.

21 Australian Federal Police, *AFP National Guideline on politically sensitive investigations*, https://www.afp.gov.au/sites/default/files/PDF/IPS/AFP%20National%20Guideline%20on%20politically%20sensitive%20investigations.pdf.

Legal, the CDPP, the Attorney-General's Department, or, on referral from AFP Legal, the Australian Government Solicitor.

1.30 The procedures mandated in the National Guideline enable parliamentarians to raise claims of privilege in relation to seized material, and respect the rights of the relevant House to determine those claims. Material subject to a claim is temporarily withheld from investigation and material determined to be privileged is returned to the parliamentarian. The execution of the warrant provides the trigger for a member or senator to avail themselves of these protections and for the relevant House to conduct any necessary oversight.

1.31 By contrast, covert intrusive powers are exercised without the knowledge of the target of the investigation. It is generally acknowledged that the integrity and efficacy of investigations by law enforcement and intelligence agencies often depend on the secrecy that surrounds the exercise of such powers. However, this inherent secrecy means it is unclear how a Member of Parliament might raise a claim of parliamentary privilege in such circumstances, or what assurance the Parliament might have that an investigating agency has had proper regard to privilege in exercising its powers.

Conduct of inquiry

1.32 The Senate referred this matter during the committee's consideration of matters relating to claims of parliamentary privilege made over documents seized under search warrant from both a senator's office and the home of a staff member. The committee provided the Senate with a preliminary report (163rd Report) on this matter in December 2016 which set out the task before it and how it intended to proceed with it. The second report (164th Report), tabled in March 2017 reached the conclusion, accepted by the Senate, to uphold the claim of privilege. It also reported on its consideration of a matter of improper interference that had arisen in the context of the execution of the search warrant. Both these reports are significant to this inquiry as they demonstrate practical examples of the matters under consideration.

1.33 In its 164th Report, the committee, commenting on the possible contempt, flagged its work on this inquiry noting:

> … if it is to meet its stated purpose, the [National Guideline] must be revised to ensure that all persons involved in the execution of warrants understand and respect the requirement to quarantine information while claims of privilege are determined. This is a matter the committee will consider in its inquiry on the adequacy of parliamentary powers in the face of intrusive powers.[22]

1.34 The committee also held discussions with its House of Representative counterpart, the Standing Committee on Privileges and Members' Interests. Following the initial discussions this committee resolved that:

22 Committee of Privileges, *Search warrants and the Senate*, 164th Report, March 2017, p. 19.

> where a matter arises that is subject to an inquiry by both the Senate Committee on Privileges and the House of Representatives Committee on Privileges and Members' Interests, or where a matter arises in which both a Senator and a Member of the House of Representatives have made claims of privilege, the two committees will confer at the commencement of the inquiry process.

1.35 The committee sought submissions from the 20 agencies which have a statutory authority to exercise intrusive powers to assist in investigations, as well as state and territory parliaments and other comparative national parliaments. The list of submitters is in Appendix 1. The committee also had a number of private briefings from organisations.

1.36 The committee appreciates the work and interest demonstrated by those who submitted and gave briefings. It acknowledges that operation parliamentary privilege in the context of intrusive powers is a subject that does not stimulate commentary outside parliament and encourages wider discussion following this report.

1.37 Chapter 2 explores the evidence received during the inquiry and parliamentary privilege, while chapter 3 considers whether a new protocol is required to ensure that members of Parliament have an opportunity to make claims of parliamentary privilege and have those claims resolved when intrusive powers are used.