The Senate

Committee of Privileges

Parliamentary privilege and the use of intrusive powers

168th Report

March 2018

ISBN 978-1-76010-755-0

This document was printed by the Senate Printing Unit, Parliament House, Canberra.

MEMBERS OF THE COMMITTEE

Senator the Hon Jacinta Collins (**Chair**) (Victoria)

Senator the Hon Ian Macdonald (**Deputy Chair**) (Queensland)

Senator the Hon Eric Abetz (Tasmania)

Senator the Hon Richard Colbeck (Tasmania)—*from 12 February 2018*

Senator Kimberley Kitching (Victoria)—*from 29 November 2017*

Senator Nick McKim (Tasmania)—*from 9 August 2017*

Senator the Hon Lisa Singh (Tasmania)

Senator Dean Smith (Western Australia)

Former members:

Senator the Hon Bridget McKenzie (Victoria)—*to 5 February 2018*

Senator Gavin Marshall (Victoria)—*to 29 November 2017*

Former Senator Scott Ludlam (Western Australia)—*to 14 July 2017*

Committee contact details

Committee of Privileges
The Senate
PO Box 6100
Parliament House
CANBERRA ACT 2600

Telephone: (02) 6277 3360
Facsimile: (02) 6277 3199
Email: priv.sen@aph.gov.au
Internet: www.aph.gov.au

Table of contents

A separate volume of submissions to the inquiry accompanies this report.

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.

Chapter 2

Key issues raised in the inquiry

2.1 The committee has been asked to report on whether existing protocols for the execution of search warrants on the premises of members of Parliament ('Members') sufficiently protect the capacity of Members to carry out their functions without improper interference. This chapter summarises some of the key issues raised in the evidence, including:

- the scope for updating the existing National Guideline in relation to search warrants;
- the extent to which parliamentary privilege applies to the actual exercise of intrusive powers;
- the extent to which the exercise of covert intrusive powers is likely to raise issues of parliamentary privilege;
- existing oversight and accountability mechanisms as they relate to the exercise of intrusive powers where issues of parliamentary privilege may be involved;
- considerations specific to access to 'metadata'; and
- the importance of preserving the integrity and efficacy of law enforcement and intelligence investigations.

Search warrants and the National Guideline

2.2 In the Commonwealth jurisdiction, the extent to which parliamentary material is protected from seizure under search warrant is governed by a settlement between the Parliament and the Executive Government.[1] This was prompted in part by the experience of members of both Houses being subjected to search warrants, with the catalyst being the Federal Court's disavowal of jurisdiction in *Crane v Gething* (2000) 97 FCR 9. The Court held that it could not make a finding relating to parliamentary privilege because the execution of search warrant was an executive act, not a judicial proceeding.[2] It was a matter for the Senate and the executive to resolve.[3] The MoU put in place processes to resolve such claims.

2.3 The MoU underpins the *National Guideline for the Execution of Search Warrants where Parliamentary Privilege may be involved* ('National Guideline'). The National Guideline sets out the process to be followed where the AFP proposes to

---

1 Senate Committee of Privileges, 164th report, March 2017, paragraph 2.1.

2 Clerk's Office, *Background Paper: Parliamentary Privilege and Execution of Search Warrants on Members' Premises—Determination of Claims of Privilege*, tabled by the President on 30 August 2016 and reproduced in Appendix A of the committee's 163rd Report, p. 1.

3 *Odgers' Australian Senate Practice*, 14th Edition, pp. 62-63.

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. It is:

> …designed to ensure that search warrants are executed without improperly interfering with the functioning of Parliament and that Members and their staff are given a proper opportunity to raise claims for parliamentary privilege or public interest immunity in relation to documents or other things that may be on the search premises.[4]

2.4 It provides guidance in relation to the procedure to be followed prior to obtaining a search warrant, prior to executing the warrant, in the actual execution of the warrant, and if a claim of privilege is claimed. The National Guideline further sets out obligations on the executing officer at the conclusion of a search.

2.5 The National Guideline provides that the AFP officer seeking the search warrant should first seek approval at a senior level within the AFP. If approval is given, the officer should in turn consult the office of the appropriate Director of Public Prosecutions (for Commonwealth offences, this would be the CDPP), who can 'provide assistance to draft the affidavit and warrant and can provide any legal advice required in relation to the execution of the warrant'.[5]

2.6 The MoU stipulates that both the President of the Senate and the Speaker of the House of Representatives will be consulted when the AFP revise and reissue the National Guideline. To date there has been no consultation. However, the AFP has put in place additional procedures that are required to be followed when investigations of serious crimes relate to members of Parliament. These additional procedures relate to both actions taken on initial referral and 'the subsequent approvals to take investigative steps'.[6] These procedures are set out in an associated document: the AFP's *National Guideline on Politically Sensitive Investigations*.[7]

2.7 The right to claim parliamentary privilege in relation to the execution of search warrants does not derive from the MoU and National Guideline. It adheres to material closely connected to parliamentary proceedings by reason of the Commonwealth Parliament's inheritance of the House of Commons powers, privileges and immunities. Therefore, the National Guideline should not be viewed as providing any particular authority to make such claims; rather it guides officers of the executive arm of government in their interactions with members of parliament.

---

4 Preamble of the *National Guideline for the Execution of Search Warrants where Parliamentary Privilege may be involved*, as reproduced in Appendix A of the Committee of Privileges 163rd report.

5 Paragraphs 5.1 and 5.2 of the National Guideline.

6 Australian Federal Police, *Submission*, pp. 12 -13.

7 https://www.afp.gov.au/sites/default/files/PDF/IPS/AFP National Guideline on politically sensitive investigations.pdf.

Updating the National Guideline to account for technological change

2.8 Evidence received would suggest that while the National Guideline is essentially sound, there is scope for updating it to ensure it remains relevant in light of technological changes, including the shift toward electronic storage and filing systems. In particular, the AFP expressed support for the notion of updating the National Guideline to ensure it 'continues to provide adequate guidance and appropriate instruction for protecting parliamentary privilege in today's environment'.[8]

2.9 The committee notes that in recent years there have been both legislative and technological changes which are reflected in how the AFP obtains materials under search warrants, how it collates those materials and how they are secured within the AFP's systems.

2.10 There would also appear to be scope and support for updating the National Guideline to cover the use of constables assisting in the execution of search warrants. 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.[9]

2.11 The AFP in acknowledging the committee's report indicated that those who are involved in the execution of search warrants should 'understand and respect the requirements around use and disclosure of information while claims of parliamentary privilege are being determined'.[10]

Intrusive powers and parliamentary privilege

2.12 A range of views were expressed in submissions regarding the interface between intrusive powers and parliamentary privilege. Differences related less to the extent to which parliamentary privilege limited the use of material obtained through intrusive powers, but more to the degree that parliamentary privilege should or could constrain the actual use of intrusive powers when materials constituting 'proceedings in Parliament' were involved.

2.13 The fact that parliamentary privilege limits the use by a court or tribunal of materials that are part of 'proceedings in Parliament' is not disputed; this 'use immunity'—that is, a rule relating to the use to which evidence may be put—is largely codified in section 16 of the *Parliamentary Privileges Act 1987*. However, 'use immunity' is only one element of privilege.

---

8 Australian Federal Police, *Submission*, p. 12.

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

10 Australian Federal Police, *Submission*, pp. 11–12.

2.14 The focus on the 'use immunity' aspect of parliamentary privilege is distracting and disconnects it from its raison d'être. *Odgers' Australian Senate Practice* sets out the reasons thus:

> Parliamentary privilege exists for the purpose of enabling the Senate effectively to carry out its functions. The primary functions of the Senate are to inquire, to debate and to legislate, and any analysis of parliamentary privilege must be related to the way in which it assists and protects those functions.[11]

2.15 Parliamentary privilege is both a set of immunities and a set of powers. This duality is acknowledged in the National Guideline in stating its purpose:

> This guideline is designed to ensure that AFP officers execute search warrants in a way which does not amount to a contempt of Parliament and which gives a proper opportunity for claims for parliamentary privilege or public interest immunity to be raised and resolved.[12]

Covert intrusive powers and parliamentary privilege

2.16 The AFP expressed some scepticism regarding the potential for its exercise of intrusive powers to have a chilling effect on the work of the parliament and its members. For example, in relation to its powers to access information held by parliamentary departments, departments of state or private agencies, the AFP noted that police inquiries remain secret unless and until their results are used in a criminal prosecution, and the public has confidence in the AFP fulfilling its statutory obligations in regard to enforcing the criminal law. On this basis, the AFP argued that its exercise of such powers 'do not have any "chilling effect" on parliamentary free speech'. The AFP further argued that its use of covert intrusive powers, in contrast to the execution of search warrants, would be unlikely to disrupt the work of a Member's office or impede the ability of constituents to communicate with a Member, precisely because they are covert.[13]

2.17 In making this argument, the AFP observed that there is no ' ... judicial authority for parliamentary privilege so as material or information is immune from the exercise of police functions and powers'.[14] As such, in the AFP's analysis the operation of parliamentary privilege as a rule of evidence—that is, as a 'use immunity'—is not affected by its exercise of covert intrusive powers.[15] The AFP

---

11 *Odgers' Australian Senate Practice*, 14th Edition, p. 42.

12 *National Guideline for the Execution of Search Warrants where Parliamentary Privilege may be involved*, as reproduced in Appendix A of the Committee of Privileges 163rd report, p. 27.

13 Australian Federal Police, *Submission*, p. 22.

14 The AFP noted that rather than any judicial authority, the basis for the prevention of privileged material being seized under a search warrant is through the agreed terms of the MoU on the execution of search warrants on the premises of members. Australian Federal Police, *Submission*, p. 7.

15 Australian Federal Police, *Submission*, pp. 22–23.

concluded that it considers that current arrangements 'allow police to conduct covert investigations into serious criminal matters, while maintaining parliamentary privilege over any privileged material so obtained'.[16]

2.18 In contrast, the President of the NSW Legislative Council submitted that there is good cause to believe that any use of covert intrusive powers has 'the potential to curtail the free and ready flow of information to members, issues of privilege may arise, albeit that such activities by their very nature would presumably not often enter into the public domain'.[17]

2.19 Section 16 of the Privileges Act applies aspects of the inherited provisions of Article 9 of the Bill of Rights, 1688 to the Australian context, and subsection (2) defines 'proceedings in Parliament'. In her background paper, the former Clerk noted that section 16 is regarded as a correct codification of the existing law, indicating that 'Its validity was affirmed by the Federal Court in *Amman Aviation Pty Ltd v Commonwealth* (1988) 19 FCR 223'.[18] The former Clerk continued by stating that 'neither Article 9 nor section 16 is confined to documents' and advising the committee to consider in the context of making an assessment as to whether privilege might apply to documents seized from a senator and his staff:

> Whether there may be a basis for a claim of privilege and possibly for resisting compulsory process, such as seizure under search warrant, if the impact of the seizure would involve improper interference with legislative activities, regardless of the use to which the documents may be put. The concept at stake is the protection of members' sources and the chilling effect on the provision of information to members of Parliament recognised by McPherson JA in *Rowley v O'Chee*:
>
> > Proceedings in Parliament will inevitably be hindered, impeded or impaired if members realise that acts of the kind done here for the purposes of Parliamentary debates or question time are vulnerable to compulsory court process of that kind. That is a state of affairs which, I am persuaded, both the Bill of Rights and the Act of 1989 are intended to prevent. (*O'Chee v Rowley* (1997) 150 ALR 199 at 215).[19]

2.20 In undertaking the current inquiry, the committee queries why the same principle should not apply to material (in whatever form) obtained through the use of covert intrusive powers. The lawful use of covert intrusive powers can have a chilling

---

16 Australian Federal Police, *Submission*, p. 23.

17 NSW Legislative Council, *Submission*, p. 6.

18 Clerk's Office, *Background Paper: Parliamentary Privilege and Execution of Search Warrants on Members' Premises—Determination of Claims of Privilege*, tabled by the President on 30 August 2016 and reproduced in Appendix A of the committee's 163rd Report, p. 6.

19 Clerk's Office, *Background Paper: Parliamentary Privilege and Execution of Search Warrants on Members' Premises—Determination of Claims of Privilege*, tabled by the President on 30 August 2016 and reproduced in Appendix A of the committee's 163rd Report, p. 7.

effect on the work of the parliament. Any suggestion that privilege diminishes because a covert intrusive power is used to access material is inconsistent with the view that privilege should operate to protect against the chilling effects that the executive's exercise of its powers can have on the parliament. The purpose of privilege is to protect Members pursuing the duty they have to scrutinise legislation and make government accountable and transparent. How material relating to the work of a parliamentarian is accessed is not determinative as to whether a question of privilege is enlived.

Current oversight mechanisms

2.21 Another aspect of the AFP's submission went to the oversight mechanisms in place for both the use of intrusive powers and the storage and use of any material obtained in the exercise of the powers. It argued that its use of covert intrusive powers is currently subject to 'robust oversight and accountability mechanisms', including internal governance arrangements to ensure legislation is followed and record keeping and reporting obligations are met, external scrutiny by the Commonwealth Ombudsman, and scrutiny by the courts.[20] The suggestion is that these mechanisms act as safeguards to ensure that questions of parliamentary privilege are not overlooked.

2.22 However, the Ombudsman has advised that in performing its statutory compliance audits of law enforcement agencies, it currently does not consider the implications for parliamentary privilege in the operation of the relevant legislation.[21] The Ombudsman further explained that its audits are generally in relation to powers used to investigate a criminal offence and 'provide protections for unnecessary and unwarranted privacy intrusion for all members of the public, including Parliamentarians'.[22] In making this point, the Ombudsman's submission arguably, albeit perhaps inadvertently, suggests an equivalence between the protections afforded by parliamentary privilege and more general privacy protections.

2.23 The Ombudsman also advised that the scope and focus of its oversight role is prescribed in the legislation, and this currently does not extend to considering parliamentary privilege. The Ombudsman concluded that amendments to legislation can change this scope and focus, and when this occurs, 'we adjust our audit methodology accordingly'.[23] The Ombudsman would not consider the implications for parliamentary privilege in its audits unless it was directed to do so either by legislation or another mechanism such as a request for an inquiry.

2.24 The Inspector-General of Intelligence and Security (IGIS) has a similar oversight role in relation to Australian intelligence agencies. In its submission, IGIS explained that it regularly examines selected agency records to 'ensure that the

20 Australian Federal Police, *Submission*, p. 17.

21 Commonwealth Ombudsman, *Submission*, p. 2.

22 Commonwealth Ombudsman, *Submission*, p. 2.

23 Commonwealth Ombudsman, *Submission*, p. 2.

activities of the intelligence agencies comply with the relevant legislative and policy requirements'. Parliamentary privilege, it advised, raises issues of both legality and propriety: IGIS could, for example, consider compliance with the Privileges Act, or whether agency 'policies and procedures pay sufficient regard' to parliamentary privilege.[24]

2.25 There is little in the evidence received to suggest that parliamentary privilege is given any particular consideration through the existing oversight and accountability mechanisms that apply to the use of covert intrusive powers.

2.26 It is significant that to the extent that issues of parliamentary privilege might be considered through existing oversight and accountability mechanisms that apply to the exercise of covert intrusive powers, this would only happen *after* a power has been exercised. There is no mechanism to ensure accountability and no oversight to identify possible improper interferences and potential contempts that may have occurred through the exercise of an intrusive power. Nor is there any indication at what point or how a member could make a claim of privilege relating to the information collected, or of a process as to how such a claim may be resolved.

Considerations specific to metadata access

2.27 In the Senate, the view was expressed that this inquiry was about the implications of the metadata preservation and access regime for the privileges and immunities of members of Parliament. Amendments to the TIA Act made by the *Cybercrime Legislation Amendment Act 2012* and the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* created a preservation and access regime for stored communications and obligations on carriage service providers to store certain data (that is, 'metadata') for certain periods of time. While these amendments significantly enhanced the ability of law enforcement and intelligence agencies to access new sources of information, they made no particular provision for the protection of members of Parliament. This, in itself, is not unusual. The law of parliamentary privilege is of general operation and applies without being specifically acknowledged in individual laws. Nonetheless, this recent expansion of intrusive powers does raise questions regarding the adequacy of existing safeguards to protect the ability of members of Parliament to carry out their functions without possible improper interference.

2.28 The AFP contended that parliamentary privilege is more likely to apply to the content of communications as opposed to the metadata about those communications.[25] The AFP's reasoning here was based on its view that privilege is primarily concerned with protecting the content of communications from impeachment or questioning.

2.29 However, even allowing that metadata lacks 'content' (a proposition that is questionable) concerns have been raised that the exposure of a member's metadata to the intrusive powers of law enforcement and intelligence agencies could have a

24 Inspector-General of Intelligence and Security, *Submission*, pp. 6–7.

25 Australian Federal Police, *Submission*, p. 22.

chilling effect on the work of the parliament. For example, as the submission from the Clerk of the House of Commons (United Kingdom) noted, some MP's have raised concerns that 'the ability of the police and intelligence services to access MPs' metadata would inhibit their ability to hold the Government to account by potentially identifying whistleblowers'.[26] One such case referred to in the Clerk's submission concerned the use of metadata in the investigation of a leak of information by a civil servant to Mr Damian Green MP, Member for Ashford. The investigation ultimately led to the arrest of Mr Green, and the importance of certain metadata in this case was a cause for concern for some members. Mr David Davis MP captured these concerns, telling the House of Commons:

> The collection of metadata cripples whistleblowers, because it tells us precisely who has talked to whom, when and where. Metadata tracking led to the arrest of my right hon. friend the Member for Ashford. That area is material to the operation of holding the Government to account.[27]

2.30 In a 2013 submission to the New Zealand Privileges Committee's inquiry into the question of privilege regarding the use of intrusive powers, former Clerk of the House of Commons (United Kingdom), Sir Robert Rogers KCB, wrote that parliamentary privilege in effect applied to metadata in the same way it applied to 'content'. This, he explained, reflected the fact that metadata could be 'very revealing about individuals and organisations', and in some situations 'even more revealing than content':

> Our approach to metadata such as e-mail or telephone logs is fundamentally the same as for data which might be regarded as substantive content (such as the body of an email, or the voice recording of a telephone conversation). Some such metadata may be virtually meaningless on its own but, when combined with other data (whether other metadata or substantive data), it may become part of a more significant data set. Such aggregation may have the effect of turning non-personal data into part of a personal data set, or turning non-sensitive data into a sensitive data set. A simple example would be the time-stamps on e-mails, when added to the core data.[28]

2.31 A similar position was put by the Clerks of the Parliament in Australia in their submission to the same New Zealand inquiry:

> There is no reason for metadata (or any other sets of information held on parliamentary information and security systems) to be treated differently from other information. The underlying concern is to ensure that parliamentary privilege is considered as part of any request for information – the format of that information is not relevant.

---

26 Clerk of the House of Commons (United Kingdom), *Submission*, p. 2.

27 Clerk of the House of Commons (United Kingdom), *Submission*, pp. 2–3. The case against Mr Green did not proceed, due to 'insufficient evidence'.

28 Sir Robert Rogers KCB, Clerk of the House of Commons, United Kingdom, Submission to the New Zealand House of Representatives Privileges Committee, 31 October 2013, p. 10.

> It may theoretically be possible to categorise some sets of information (e.g. particular types of data) as being administrative, technical, or otherwise unlikely to raise issues in relation to parliamentary privilege, however any process designed to pre-identify sets of information that may or may not attract parliamentary privilege is fraught with difficulty – instead, it is best to consider issues of parliamentary privilege on a case-by-case basis as requests for information are received.[29]

2.32 In considering the implications of metadata domestic preservation orders on the privileges and immunities of members of Parliament, the committee notes that at present there is little if any transparency regarding when an investigating agency has accessed or sought to access a member's metadata. In responding to questions taken on notice at Additional Estimates in February 2016, the AFP declined to advise if any parliamentarians have been subject to an AFP initiated metadata domestic preservation order, and pointed to 'operational security reasons' that prevent it from providing advice on preservation orders in relation to classes of particular persons. The AFP further advised that the total number of preservation orders and revocations made by the AFP in a given year, and the number of telecommunications data disclosure authorisations made by the AFP in that year, is publicly reported. However, the AFP also observed that it is an offence under the TIA Act to communicate specific preservation notice information to another person, as it is to disclose whether an authorisation to access telecommunications data has been, or is being, sought. 'It is also an offence', the AFP continued, 'to disclose information about the making of a Division 4 authorisation, the existence or non-existence of such an authorisation, the revocation of such an authorisation, or the notification of such a revocation'.[30]

2.33 The lack of transparency in relation to metadata access presents a problem. To the extent that access by law enforcement and intelligence agencies to certain metadata might be said to have amounted to an improper interference with the free exercise by a House or committee of its authorities or functions, or with the free performance by a member of the member's duties as a member, then the access to this metadata could be dealt with as a potential contempt, even if such access was otherwise lawful. Yet as it stands, it is highly unlikely that information on the extent to which members of Parliament and their staff have been subjected to metadata access orders will be made public or otherwise made available to members of Parliament, let alone brought to the attention of members whose metadata may have been accessed.

Preserving the efficacy and integrity of investigations

2.34 A number of law enforcement and intelligence agencies were keen to impress upon the committee the need to preserve the flexibility and efficacy of their

---

29 Mr Richard Pye, Acting Clerk of the Senate, and Mr Bernard Wright, Clerk of the House of Representatives, Submission to the New Zealand House of Representatives Privileges Committee, 11 November 2013, p. 3.

30 Australian Federal Police, responses to Question on Notice AE16/059, 27 September 2016.

investigative activities. These submissions argued that efforts to strengthen the protections provided by parliamentary privilege in relation to the use of intrusive powers should be weighed against the need to ensure the integrity of investigations.

2.35 Arguing that existing oversight mechanisms in relation to the use of intrusive powers were sufficient to protect parliamentary privilege, the AFP submitted that 'to the extent additional oversight would add time and delay, it may come at some cost, both financially, and in terms of the AFP's efficacy and perceived integrity as an independent agency'.[31]

2.36 The AFP also referred to the 'practical difficulty' in distinguishing between privileged and non-privileged material, and cautioned that restrictions on evidence gathering 'would have the detrimental effect of assisting wrongdoers in the concealment of their criminal activity'.[32]

2.37 While ASIO did not refer to any specific tension between its operational efficacy and potential new measures to protect parliamentary privilege, it did emphasise the importance of considering the matters raised by the terms of reference in the context of threats from hostile foreign actors. It noted, in this regard, that parliamentarians are 'not immune from the attention of foreign states', and indeed are likely 'aspirational targets for those who engage in politically motivated violence'.[33] This could be read as a caution that measures designed to protect the integrity of parliament could prove counterproductive, to the extent such measures hinder ASIO's ability to investigate the activities of hostile foreign actors targeting the parliament and its members.

2.38 ACLEI used its submission to note the care taken by Australian parliaments and their respective privileges committees to 'ensure that the criminal law is able to apply equally to elected members of parliament, as it would to any other Australian'.[34] While this statement is unremarkable, it serves as a reminder that any new mechanism to strengthen the application of parliamentary privilege in relation to the use of intrusive powers should not serve to make parliamentarians any less accountable before the law.

2.39 For its part, the AFP was more explicit in this regard, submitting that it was of 'obvious importance that parliamentary privilege should not impede the investigation of offences committed by serving members of Parliament'.[35]

2.40 Any protocol relating to the exercise of intrusive powers and parliamentary privilege should have proper regard to the fact that the ability to exercise intrusive

---

31 Australian Federal Police, *Submission*, p. 9.

32 Australian Federal Police, *Submission*, p. 16.

33 Australian Security Intelligence Organisation, *Submission*, p. 4.

34 Australian Commission for Law Enforcement Integrity, *Submission*, p. 2.

35 Australian Federal Police, *Submission*, p. 9.

powers, and to do so covertly when appropriate, is an important part of the law enforcement and intelligence toolkit.

2.41 Equally, instances where matters of parliamentary privilege are raised by the exercise of intrusive powers are likely to be rare. To the extent that law enforcement and intelligence agencies are required to follow additional processes in their exercise of intrusive powers under a protocol, any associated costs in time or resources needs to be weighed against the likelihood that such processes would only be necessary on a very occasional basis.

CCTV and access control system data at Parliament House

2.42 The difficulties with the argument offered by the AFP and others suggesting that if a Member is not aware of the intrusion there can be no effect on the Parliamentary work, was evident in the committee's inquiry into the use of CCTV material in Parliament House. In that instance - a matter of a possible contempt - the argument that was put that as 'the investigators were unaware they were witnessing something connected to parliamentary business, they could not be not be said to be obstructing it, and certainly not knowingly'.[36] The merits of the argument were not explored by the committee because of other evidence, but it did express concern and made a recommendation around the development of a new Code of Practice that 'emphasises accountability to the Presiding Officers …'.[37]

2.43 During this inquiry the committee reviewed the development of the new policies relating to the closed-circuit television (CCTV) system and those for any proposed systems to access private area systems at Parliament House and in particular the release of CCTV footage and stored data from the private area access system.

2.44 The committee understands that the approval of the Presiding Officers would be required for any release of data which may have implications for parliamentary privilege and which is maintained by either system. Because the Presiding Officers would have a role in approving the release of CCTV footage where parliamentary privilege may be involved, or the release of access control data which pertains to a Senator or Member, it would appear that proper consideration would be given to parliamentary privilege if such material was subject to the exercise of an intrusive power.

Conclusion

2.45 Evidence received suggests that there is scope to both update the existing protocol in relation to the execution of search warrants, and to expand the protocol to cover the exercise of a broader range of intrusive powers when matters of parliamentary privilege may be raised. This evidence suggests growing uncertainty regarding the operation and application of parliamentary privilege in relation to the exercise of intrusive powers. In part, this uncertainty derives from recent changes in

36 Committee of Privileges 160th Report, December 2014, p. 15.

37 Committee of Privileges 160th Report, December 2014, p. 38.

technology and related shifts in investigative practice, including the increasing use of covert intrusive powers by law enforcement and intelligence agencies. These covert intrusive powers include communication intercepts, electronic surveillance, access to stored communications and access to stored telecommunications data. It is possible the National Guideline could be relevant in the instance the AFP sought a warrant to access the telecommunications content of a Member, or a warrant to use a surveillance device in relation to the communications or activities of a Member. However, none of the evidence received by the committee suggests that it is considered in the exercise of any warrant other than those that are executed on physical premises. Further the National Guideline does not extend to the access of metadata, or other information held by parliamentary departments, departments of state or private agencies in relation to members of Parliament and their staff.

2.46 Finally the evidence indicates that none of the current oversight mechanisms of the exercise of covert intrusive powers, including those examining the storage and access of the information garnered in the use of those powers consider the question of parliamentary privilege.

Chapter 3

Is a new protocol required?

Introduction

3.1 Evidence considered by the committee indicates the absence of any consideration as to how questions of parliamentary privilege may be resolved in the exercise of covert intrusive powers, and that the provisions of the National Guideline are limited to warrants that are executed on physical premises. In addition, there is a lack of evidence that any consideration is given as to whether the information collected where a warrant is not required raises questions of parliamentary privilege and how such questions should be resolved. Current oversight mechanisms are also blind to any questions of privilege.

3.2 The task the committee has been given is to ascertain whether the work of the Parliament is sufficiently free from possible improper interference given the technological and legislative developments in recent years. The purpose of parliamentary privilege, both in terms of immunities and powers, is to ensure that parliamentarians can hold governments to account and undertake their legislative duties. The purpose of the powers that have been legislated under the TIA Act and the SD Act are to facilitate those in law enforcement and intelligence agencies to ensure that they can do the work with which they are tasked. As the world of information storage and access becomes increasingly virtual, the technology available to law enforcement and intelligence agencies has expanded into new spheres and so have their powers. How do the protections afforded by privilege to parliamentarians so that they can undertake their duties free from improper interference operate in this environment?

3.3 This chapter considers first the existing protocols as set out in the MoU and the National Guideline, before considering the use of intrusive powers and the implications for parliamentary privilege.

Current protocols for the execution of search warrants

Opportunities to make claims of parliamentary privilege and have those claims resolved

3.4 The current protocols as embodied in the MoU and the National Guideline have operated for over a decade. In 2016, the first determined claims of parliamentary privilege under the protocols were made by a senator over material, largely documents, which were seized during the execution of a search warrant. Those claims were resolved by the Senate, following a report by this committee. In addition to the recommendation relating to the privilege claims, the committee recommended that the Senate:

> note the requirement for remedial action in relation to the national guideline for the execution of search warrants where parliamentary privilege may be

> involved, which the committee will address in its inquiry into intrusive powers.[1]

3.5 The recommendation arose from the possible contempt matter investigated by the committee and reported together with the matter of privilege as the two matters were related. In investigating the possible contempt the committee was made aware of the use of a mobile phone by a 'constable assisting' to take snapshots of documents before transmitting the snapshot to other officers within the same agency for advice. The committee did not make a contempt finding. However, it was alerted to a possible need to update the National Guideline which was negotiated prior to such practices becoming commonplace. The AFP's evidence supported an update to '… address the use of constables or third parties assisting in the execution of search warrants ...'.[2]

3.6 The incident reveals not only that the National Guideline does not envisage the use of third parties to provide technical assistance but those who provide that assistance are not provided with the requisite knowledge of either the terms of the protocol or the immunities and powers provided by parliamentary privilege.

3.7 The National Guideline indicates that:

> It is not always easy to determine whether a particular document falls within the concept of 'proceedings in parliament'. In some cases the question will turn on what has been done with a document, or what a Member intends to do with it, rather than what is contained in the document or where it was found.[3]

3.8 It recognises the importance of providing Members with proper opportunity to make a claim of privilege and have that claim assessed and sets out that in executing a search warrant where a Member or a senior member of his/her staff is present, the executing officer 'should ensure that the Member, or member of staff, has a reasonable opportunity to claim parliamentary privilege or public interest immunity in respect of any documents or other things that are on the search premises'.[4] The National Guideline in turn sets out the procedure to be followed in the instance a claim of parliamentary privilege is made.[5]

3.9 The committee's view is that the protocol is sound in terms of the process for claims of parliamentary privilege, but it is in the practice that the process can falter. All officers engaged in the execution of search warrants should be aware of the requirements of the National Guideline. The committee considers that until there is an opportunity to consult and amend the National Guideline, this shortcoming initially could be addressed in an administrative manner, by the AFP briefing all those assisting in the execution of the warrant on the protocols set out in the National

---

1 Committee of Privileges 164th Report, p. 20.

2 Australian Federal Police, *Submission*, p. 11.

3 *National Guideline*, p. 2.

4 *National Guideline*, p. 4 (paragraph 6.7).

5 *National Guideline*, pp. 45 (paragraphs 6.10 – 6.14).

Guideline. This should be regarded as a temporary measure with the view of incorporating the requirement in the National Guideline following consultations.

The implications of the use of intrusive powers on privileges

3.10 Evidence provided by the AFP also acknowledged that the technological developments since the signing of the MoU influence not just police practices, but how information is stored, the amount of information stored and the forms in which that information is stored. They expressed the view that:

> there may be benefit in a review of the NG [National Guideline] to ensure that it continues to provide adequate guidance and appropriate instruction for protecting parliamentary privilege in today's environment.[6]

3.11 However, this view does not extend to the use of other intrusive powers covertly or otherwise. The exclusion is based on the view that an intrusion that is undetected cannot constitute an improper interference (and therefore a contempt) and the view that parliamentary privilege is limited to 'use immunity'. It is one which is shared across other agencies giving evidence about the use of these powers.

3.12 This argument is maintained despite one of the key aspects of the Parliament's powers – the ability to investigate and punish actions that it finds are improper attempts to interfere with the conduct of members and their duties – is articulated in the National Guideline. The Senate has clearly established procedures for dealing with interference or attempted interference and the National Guideline is explicit in its consideration of the need to prevent actions that could amount to a contempt in the execution of search warrants.

3.13 Further, the acknowledgement in the National Guideline that it is not always readily discernible whether a document relates to parliamentary proceedings reflects the Senate's view that the class of document does not define whether a question of privilege can be invoked. It is difficult to see how the method used to access a document or information could be determinative as to whether a question of privilege is enlivened.

3.14 The committee notes that the interception of communications and other electronic surveillance requires a warrant. Access to stored communications content and the issuance of preservation notices also requires a warrant. However, access to telecommunications data ('metadata') does not require a warrant (except where a journalists' or their employers' telecommunications data is sought for the purposes of identifying a source of the journalist). Any information relating to the proceedings of parliament gained from those activities should be able to be subject to a claim of parliamentary privilege and the committee considers that there should be a clear mechanism by which those claims can be resolved. However, although warrants are generally required, there is no evidence to indicate that that any of the procedures required by the National Guideline are considered to apply in this context.

---

6 Australian Federal Police, *Submission*, p. 12.

3.15 The committee is of the view that under current arrangements there is reason to question whether Members are provided with any opportunity to make claims of privilege in relation to the exercise of intrusive powers other than search warrants, particularly when those powers are covertly exercised. Consequently the committee has concluded that the existing protocols are not sufficient to protect the work of the Parliament from possible interference.

Intrusive powers, current oversight regimes and acknowledgement of Parliamentary Privilege

3.16 The committee notes that there was little in the way of evidence provided during the inquiry that suggests that there is any acknowledgment of parliamentary privilege in any of the oversight mechanisms that are currently operating.

3.17 Further it would appear to the committee that despite the AFP's *Guideline on Politically Sensitive Investigations*, which reminds investigators of the need to consider parliamentary privilege, the storage of metadata information is such that there is no consideration given to where that information has been sourced, unless it relates to the interception of the journalist's metadata. The AFP was unable to indicate to the committee whether any such information relating to members or senators or their staff had been collected, as their systems were not designed to provide this information.

Specific protocols

3.18 The committee is concerned that there are no protocols in place and no practices observed in relation to the intrusive powers where matters of parliamentary privilege may be involved. The notion that questions of privilege are not relevant because the parliamentarian does not know that the intrusive powers have been exercised are equally concerning. There is clear evidence cited in the Clerk of the United Kingdom House of Commons' submission that material collected in such exercises can be established to invoke claims of parliamentary privilege. The question for the committee is how such claims can be made and resolved in practice.

3.19 In considering this question the committee is cognisant that there are different elements at play both for intelligence and law enforcement agencies using the intrusive powers and the Parliament. For the intelligence and law enforcement agencies, intrusive powers are an important part of their investigative toolkit, while the protections against improper interference offered by parliamentary privilege are central to the work of the Parliament.

3.20 The committee heeds the message in ASIO's submission that '… Parliamentarians are not immune to the attention of foreign states; …'[7] and does not seek to confer any general immunity on Members, nor place evidential material beyond the reach of agencies simply because that material originated with or is in the possession of a Member. It accepts that the purpose of privilege is enable the

7 Australian Security Intelligence Organisation, *Submission*, p. 4.

Parliament, its committees and Members to carry out their functions without improper interference, and to deal with any such interference or attempted interference. The committee accepts that not all material or information held by a Member requires the protection of parliamentary privilege simply because that material or information was created by or is in the possession of a Member.

3.21 However, as argued in another sphere by Mr Bret Walker SC, privilege is not for the protection of members, but the institution:

> Seen in that light – and that's the traditional and contemporary understanding of the purpose of parliamentary privilege – an entrenchment on it is in reality a reduction in the efficacy of the system of parliamentary government, which is for the people, not the parliamentarians.[8]

3.22 The committee is of the view that the best way to resolve the tension between those exercising intrusive powers and the parliament is the development of agreed protocols between the relevant parties.

Use of intrusive powers under warrant

3.23 In considering what features any such protocols might have, the committee found it useful to draw a distinction between those powers that are exercised subject to a warrant and those that can be exercised without a warrant. The value of this distinction from the committee's perspective is that there is an existing set of agreed protocols already in operation in relation to the execution of search warrants where questions of parliamentary privilege might arise. The successful operation of these processes as set out in the MoU and the National Guideline provides a useful template for the development of further guidelines to be used in the execution of warrants where intrusive powers are deployed.

Quarantine and review of material obtained through intrusive powers

3.24 One of the key features of the existing processes that the committee considers should be incorporated into any new protocol is a process to quarantine and review material or information that may give rise to parliamentary privileges issues where the information has been obtained through intrusive powers.

3.25 Where a Member's communications are intercepted, or where material or information in the possession of a Member is sought or obtained through the exercise of intrusive powers, it would be preferable where possible to provide that Member with an opportunity to review the material in question. If the Member considers the material part of proceedings in Parliament, they would then be able to make a claim of privilege and have that claim assessed. The material or information should remain quarantined until that claim had been assessed. It would only be provided to law enforcement and intelligence agencies if any claim of privilege were rejected.

3.26 Where covert intrusive powers are exercised, the process would still be relevant in cases of what could be termed 'collateral intrusion'—that is, cases where a

8 Parliamentary Joint Committee on Intelligence and Security, *Hansard*, 16 February 2018, p. 5.

Member is not themselves the target of an investigation, but where their communications or material in their possession has been obtained, possibly inadvertently or unexpectedly, through an investigative process.

3.27 The committee acknowledges there may be occasions where it would prove difficult to provide a Member with an opportunity to make a claim of parliamentary privilege over material obtained through the exercise of an intrusive power. Careful consideration would need to be given as to how this process would be managed in the circumstances where a Member was themselves the subject of an investigation and where covert intrusive powers were used.

Applications for warrants and other authorisations to exercise intrusive powers

3.28 Quarantining the information subject to a claim of parliamentary privilege until the claim is adjudicated occurs after an intrusive power is exercised. It is possible that an improper interference or potential contempt could occur at the point a covert power is exercised. In developing an agreed set of processes consideration should also be given to establishing a mechanism that would ensure that law enforcement and intelligence agencies have proper regard to parliamentary privilege in the exercise of intrusive powers whether covert or otherwise. One possible mechanism is to agree to a process where the issuing authority (or the Minister in the case of ASIO) prior to authorising the warrant would need to have regard to question of parliamentary privilege and in the event that a claim of parliamentary privilege was likely to arise, additional processes in both the issuing of the warrant and its execution would be triggered.

Acting without warrant

3.29 The committee now turns to the information held by parliamentary departments, departments of state or private agencies in relation to members of Parliament or their staff which can be acquired without a warrant. This includes the information commonly referred to as metadata that is collected under the TIA Act, as well as electronic information captured in the use of such things as electronic keys. Access to such information does not necessarily require the use of intrusive powers whether covertly or otherwise as such information can be obtained during routine investigations.

3.30 In addressing the extent to which 'metadata' might be subject to the claims of parliamentary privilege, the Clerks of the Australian Parliament have argued that in considering whether parliamentary privilege relates to certain information, the format of information is ultimately irrelevant[9]. This principle serves as a response to the erroneous view that claims of parliamentary privilege cannot be found to exist in relation to 'metadata', as opposed to 'content'. The distinction between 'metadata' and 'content' is questionable. Clearly, metadata can be very revealing, and legitimate

9 Mr Richard Pye, Acting Clerk of the Senate, and Mr Bernard Wright, Clerk of the House of Representatives, Submission to the New Zealand House of Representatives Privileges Committee, 11 November 2013, p. 3.

concerns have been raised that the exposure of a Member's metadata to the intrusive powers of law enforcement and intelligence agencies could have a chilling effect on the work of the parliament.

3.31 Given the possibility of parliamentary privilege issues arising in the accessing of this type on information, the committee formed the view that agreed protocols should also be put in place to ensure a process of establishing whether there are parliamentary privilege matters that need to be raised and resolved. The difficulty in developing such protocols is finding an appropriate trigger point at which the member or their staff can make such a claim. The access to information under the terms of the TIA Act requires legal tests to be met prior to the provision of the material. The committee envisages that such points prior to accessing the information should be the point where questions of privilege become a consideration – the application of the legal tests should be regarded as mimicking the granting of a warrant. Any protocol developed which would allow information to be quarantined so that any privilege claims can be made and resolved would come into play at that point. This would allow any claims of privilege to be properly assessed prior to the material or information being used in the investigation. The committee is of the view that this should be standard practice if any of the information revealed during the investigation relates to a Member of Parliament.

3.32 A more difficult task is to establish a trigger point where such information is accessed as part of routine investigations without the use of a warrant. Finding that trigger point may not be possible, but it should not prevent the application of protocols that allow claims of privilege to be made and resolved post the access to the information and prior to its use in any inquiry.

Recommendation: The committee recommends that, to ensure claims of parliamentary privilege can be raised and resolved in relation to information accessed in the exercise of intrusive powers and other investigative powers, the Presiding Officers, in consultation with the executive, develop protocols that will set out agreed processes to be followed by law enforcement and intelligence agencies when exercising those powers.

Accountability and oversight mechanisms

3.33 The operation and effectiveness of the proposed new protocol would be enhanced by accountability and oversight mechanisms. The committee established that the current oversight mechanisms do not examine whether questions of parliamentary privilege have been enlivened as a consequence of the use of intrusive powers.

3.34 Both the agencies tasked with oversight responsibilities – in the case of law enforcement, the Ombudsman and for the intelligence community, IGIS - indicated that such matters were not currently within their remit. The committee understands that both organisations would be prepared to extend their remit if required.

3.35 The committee considers that reviews by the Ombudsman and IGIS would be useful. However, it is of the view that, where a law enforcement or intelligence agency has accessed (inadvertently or otherwise) potentially privileged material

through the exercise of an investigative power, and has not followed the process set out in an agreed protocol, these instances should be reported to either the relevant Presiding Officer or the appropriate privileges committee.

3.36 To maintain comity between the Houses, it would be appropriate for the Senate privileges committee to consider Senate-only matters, and for the House privileges committee to likewise consider matters that relate solely to the House. Where a matter arises that directly concerns both Houses, it would be open to the two committees to consider the matter jointly.

3.37 The privileges committees should also have an ongoing review function in relation to the effectiveness and appropriateness of the protocol. In this way, the committee in question would be able to provide advice in relation to any required amendments to the protocol.

Senator the Hon Jacinta Collins

Chair

Appendix

List of submissions to inquiry

1. Legislative Assembly of the Northern Territory, received 10 April 2017
2. Inspector-General of Intelligence and Security, received 11 April 2017
3. Australian Security Intelligence Organisation, received 12 April 2017
4. Australian Federal Police, received 13 April 2017
5. House of Commons Canada, received 14 April 2017
6. Legislative Council of New South Wales, received 20 April 2017
7. Legislative Assembly of New South Wales, received 8 May 2017
8. House of Commons United Kingdom, received 9 May 2017
9. Commonwealth Ombudsman, received 2 June 2017
10. Australian Commission for Law Enforcement Integrity, received 16 June 2017
11. Australian Law Reform Commission, received 20 June 2017
12. UNSW Law Society, received 25 January 2018

See the separate volume accompanying this report to view the submissions.