



Law Council
OF AUSTRALIA

Review of Item 250 of the National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022

Parliamentary Joint Committee on Intelligence and Security

21 December 2022

Table of Contents

About the Law Council of Australia	3
Introduction	4
Identification and protection of parliamentary privilege	5
Is parliamentary privilege abrogated?	6
Safeguards for parliamentary privilege	7
The United Kingdom Model	8
Safeguards on parliamentarian communications under the Investigatory Powers Act	10
Criticism of role of Prime Minister	11
Broader safeguards for sensitive information	11
Pre-collection safeguards	12
Post collection safeguards	14
The scope of proceedings in Parliament	14
The NBN Co Test	14
The scope of 'proceedings in Parliament' and metadata	15
Mechanism for asserting and resolving disputes as to parliamentary privilege	16
The role of a public interest advocate in a warrant application	17
Notification of the public interest advocate	20
Procedure for asserting privilege in the context of electronic surveillance	20
Resolving privilege disputes and the jurisdiction of the Courts	22
International Production Orders	25

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level, speaks on behalf of its Constituent Bodies on federal, national and international issues, and promotes the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

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

Through this representation, the Law Council acts on behalf of more than 90,000 Australian lawyers.

The Law Council is governed by a Board of 23 Directors: one from each of the Constituent Bodies, and six elected Executive members. The Directors meet quarterly to set objectives, policy, and priorities for the Law Council. Between Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2022 are:

- Mr Tass Liveris, President
- Mr Luke Murphy, President-elect
- Mr Greg McIntyre SC, Treasurer
- Ms Juliana Warner, Executive Member
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.asn.au.

Acknowledgment

The Law Council is grateful for the contributions of the members of the Law Council's National Criminal Law Committee and its National Security Law Working Group.

The Law Council also thanks the Privileges and Immunities Committee of its Federal Litigation and Dispute Resolution Section.

Introduction

1. The Law Council of Australia appreciates the opportunity to have appeared before the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) on 30 November 2022 in relation to its Review of Item 250 of the National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022 (**NACC Consequential Bill**).
2. The Law Council notes that it has had limited opportunity to consult with its Constituent Bodies, Sections and advisory committees in preparing this supplementary submission. As a result, this supplementary submission is provided on a preliminary basis to the Committee. The matters raised may be further discussed in due course.
3. In the course of providing evidence, the Law Council was asked to take on notice a question regarding the operation of parliamentary privilege in relation to the electronic surveillance powers engaged by Item 250 of the NACC Consequential Bill.
4. A further question was taken on notice in relation to the authorisation of International Production Orders and a warrant application by a law enforcement officer of the National Anti-Corruption Commission.
5. Each of these matters is dealt with in turn below.

Identification and protection of parliamentary privilege

6. Members of the Committee have asked related but separate questions being:
 - how can a parliamentarian assert privilege in circumstances of covert surveillance where the privilege holder is unaware of the surveillance; and
 - the Law Council's view on the proposed alternative mechanisms for the making of privilege claims and resolution of disputes.
7. As a general starting point, the Law Council recognises the important public interest protected by parliamentary privilege and its constitutional status. Section 49 of the Australian Constitution states:

The powers, privileges, and immunities of the Senate and of the House of Representatives, and of the members and the committees of each House, shall be such as are declared by the Parliament, and until declared shall be those of the Commons House of Parliament of the United Kingdom, and of its members and committees, at the establishment of the Commonwealth.¹

8. As set out in the submission of the Joint Clerks to this Committee, the relevant aspect of parliamentary privilege engaged by Item 250 of the NACC Consequential Bill is the legal immunity of freedom of speech in Parliament.
9. More precisely, the legal immunity of freedom of speech in Parliament entails the requirement that freedom of speech and debates or 'proceedings in Parliament' ought not be impeached or questioned in any Court or Place outside of Parliament. This requirement is contained in Article 9 of the Bill of Rights 1688 (UK) and is given

¹ *Australian Constitution*, s 49.

effect by section 49 of the Australian Constitution. The scope of Article 9 has subsequently been clarified by section 16 of the *Parliamentary Privileges Act 1988* (Cth).

10. Parliamentary privilege is a corollary of the separation of powers because an important requirement of an independent judiciary and legislature is that the 'legislature and the courts should not intrude into the spheres reserved to the other.'²
11. Australian Courts have described the importance of the legal immunity of freedom of speech in Parliament protected by Article 9 of the Bill of Rights in the following terms:

*For centuries, the courts have recognised that Art 9 reflects a fundamental principle of the system of government in a representative democracy that separates and demarks the exclusive jurisdiction of Parliament over its own processes from the jurisdiction that the judiciary might otherwise have had.*³

Is parliamentary privilege abrogated?

12. With respect to exercise of powers in the NACC Bill itself, clause 274 of the NACC Bill largely preserves the powers, privileges and immunities of each House of Parliament, members of each House of Parliament, the committees of each House of the Parliament, and joint committees of both Houses of the Parliament.
13. The initial question before this Committee is whether, in the absence of specific provisions relating to parliamentary privilege in the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), parliamentary privilege is implicitly abrogated.
14. The Law Council considers it doubtful that parliamentary privilege is abrogated in the context of the TIA Act for the following reasons.
15. It is a fundamental principle that the law of parliamentary privilege is not abrogated by a statutory provision 'unless the provision alters that law by express words.'⁴ Odgers on Australian Senate Practice cites the joint opinion of the then Attorney-General and the then Solicitor General:

*Whatever may be the constitutional position, it is clear that parliamentary privilege is considered to be so valuable and essential to the workings of responsible government that express words in a statute are necessary before it may be taken away ... In the case of the Parliament of the Commonwealth, s. 49 of the Constitution requires an express declaration.*⁵

16. Illustratively, subsection 37(3) of the *Auditor-General Act 1997* (Cth) is an example of the Commonwealth Parliament using express words to indicate a specific intention to abrogate parliamentary privilege under section 49 of the Australian Constitution. For instance, subsection 37(3) of the *Auditor-General Act 1997* provides that the Auditor-General 'cannot be required, and is not permitted, to

² *Buchanan v Jennings (Attorney General of New Zealand intervening)* [2005] 1 AC 115, 132 [18] (Lord Bingham) cited in *Leyonhjelm v Hanson-Young* [2021] FCAFC 22, [30] (Rares J). The privilege also operates to avoid conflicts between Parliament and the courts: *Halden v Marks* (1995) 17 WAR 447 at 463.

³ *Barilaro v Shanks-Markovina (No 2)* [2021] FCA 950, [22] (Rares J).

⁴ Odgers' Australian Senate Practice, 14th ed. 2016, 69.

⁵ *Ibid.*

disclose' specified information to the Parliament or a parliamentary committee.⁶ In this case, the Explanatory Memorandum explicitly identified an intention to abrogate parliamentary privilege:

The effect of subclause 37(3) in these respects is to act as a declaration for the purposes of section 49 of the Constitution. Where particular information is not disclosed in a public report, the Auditor-General may prepare a restricted report that includes such information to be given to the Prime Minister, the Finance Minister and the responsible Minister.⁷

17. The Law Council recognises there may be some doubt as to whether parliamentary privilege may be implicitly abrogated by general statutory provisions.⁸
18. The Law Council notes that, as a general principle, Courts will be reluctant to draw the implication of an abrogation of parliamentary privilege from a statutory scheme.⁹
19. Assuming that parliamentary privilege is formally preserved, the Law Council notes that the following concerns have been raised:
 - it is not satisfactory to allow an agency of the executive, such as law enforcement agencies, discretion to interpret the scope of parliamentary privilege in exercising its powers;¹⁰
 - the risk identified in the submission of the Joint Clerks that 'because the TIA Act is silent on the matter, there is greater risk that people may incorrectly interpret its provisions as circumscribing parliamentary privilege;¹¹ and
 - the practical value of parliamentary privilege being 'hollowed out' in the absence of effective mechanisms to notify privilege holders and assert privilege.

Safeguards for parliamentary privilege

20. The Law Council retains the view that it is appropriate to draw an analogy between its earlier submissions on the identification and protection of material subject to legal professional privilege and the current discussion on material subject to parliamentary privilege. In this context, the Law Council has consistently advocated for the following general principles underpinning statutory requirements on law enforcement applicants for electronic surveillance warrants in relation to material that may attract legal professional privilege:
 - a requirement to inform the issuing authority, as part of the warrant application, whether there are reasonable grounds to believe that privileged information would, or may be, collected as part of the surveillance activities; and if so
 - a requirement to satisfy the issuing authority that:

⁶ See more generally, Australian Law Reform Commission, [Secrecy Laws and Open Government in Australia](#) (ALRC Report 112) 16.192.

⁷ Explanatory Memorandum, Auditor General Bill 1996, [71].

⁸ See further, discussion of the advice given to the government by its legal advisers in 1990 in relation to evidence of National Crime Authority officials to the Joint Committee on the National Crime Authority. Odgers' Australian Senate Practice, 14th ed. 2016, 69-73.

⁹ Kirby J in *Sue v Hill* (1999) 199 CLR 462 at 558: "In ascertaining the Parliament's purpose in a matter connected with its privileges, no court should strain legislative language to claim a jurisdiction that has not been clearly vested in it."

¹⁰ This concern was raised by the Committee in Parliamentary Joint Committee on Intelligence and Security, [Advisory Report on the Foreign Influence Transparency Scheme Bill 2017](#) (June 2018) 113-116.

¹¹ Submission of Joint Clerks, [Review of Item 250 of Schedule 1 of the National Anti-Corruption Commission \(Consequential and Transitional Provisions\) Bill 2022](#) (1 November 2022).

- the agency has in place appropriate measures to quarantine and delete that information (without it being accessed by persons conducting the investigation); and
 - the proposed collection activity is in the public interest, having regard to the risks to privilege that access may, or is likely to, present; and
 - consideration be given to provisions requiring the agency to consider and inform the issuing authority, whether disclosure could be made to the person in whom privilege is invested without compromising the operational security or effectiveness of the investigation.¹²
21. However, the Law Council recognises that these general principles require some specification to be applied in the context of parliamentary privilege. These specifications are discussed further below in the context of pre-collection and post-collection safeguards:
- **pre-collection:** namely, at the point of authorisation to collect the information via the exercise of surveillance powers; and
 - **post-collection:** namely, in relation to the subsequent use, disclosure, handling, retention and destruction of information obtained under a surveillance warrant.
22. The Law Council considers that the issues considered by the Committee in relation to parliamentary privileged information are a subset of a broader set of issues around ensuring appropriate protections for sensitive information in the context of electronic surveillance.
23. The Law Council is supportive of incorporating additional statutory requirements, in line with the *Investigatory Powers Act 2016* (UK) (**Investigatory Powers Act**) in relation to the collection and subsequent handling of sensitive information. Additionally, the Law Council notes the specific protections for parliamentary privilege information in the UK scheme. Consideration of the UK scheme highlights the interdependence of broader safeguards for sensitive information and specific safeguards for parliamentarians.
24. The Law Council notes that section 241 of, and Schedule 7 to, the Investigatory Powers Act makes provision for the issuance of binding 'codes of practice' in relation to particular types of surveillance and information being targeted. In the UK, these codes of practice operate concurrently with long-standing norms arising from political convention, such as the political convention that the communications of parliamentarians should generally not be intercepted by law enforcement agencies, (**the Wilson Doctrine**).¹³ This approach provides greater guidance on the circumstances in which coercive law enforcement powers will be exercised in relation to parliamentarians.

The United Kingdom Model

25. In short, in the UK under the Investigatory Powers Act any interception under a warrant of communications and interference with equipment require the approval of **both** the Secretary of State and a Judicial Commissioner. Additionally, where such interference involves a parliamentarian, the approval of the Prime Minister must be

¹² Law Council of Australia, [Electronic Surveillance Reforms: Submissions on Discussion Paper](#) (18 February 2022) 39.

¹³ Pat Strickland, Joanna Dawson and Samantha Godec, Briefing Paper, [The Wilson Doctrine](#) (12 June 2017) Number 4258.

sought which partially embeds in statute the political convention known as the Wilson Doctrine.

26. The Wilson Doctrine developed from a response to questions in the House of Commons on 17 November 1966 by then Prime Minister Harold Wilson:

*With my right hon. Friends, I reviewed the practice when we came to office and decided on balance—and the arguments were very fine—that the balance should be tipped the other way and that I should give this instruction that there was to be no tapping of the telephones of Members of Parliament. That was our decision and that is our policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it.*¹⁴

27. It was subsequently clarified that the Wilson Doctrine encompasses the use of electronic surveillance by any of the three Security and Intelligence agencies and that it applies to all forms of interception that are subject to authorisation by Secretary of State warrant.¹⁵ The Wilson Doctrine was most recently restated by then Secretary of State Theresa May in the following terms:

*Obviously, the Wilson Doctrine applies to parliamentarians. It does not absolutely exclude the use of these powers against parliamentarians, but it sets certain requirements for those powers to be used in relation to a parliamentarian. It is not the case that parliamentarians are excluded and nobody else in the country is, but there is a certain set of rules and protocols that have to be met if there is a requirement to use any of these powers against a parliamentarian.*¹⁶

28. An important recent decision of the UK Investigatory Powers Tribunal found that the Wilson Doctrine has no legal effect.¹⁷ However, the Tribunal reasoned that the meaning of ‘certain set of rules and protocols’ needing to be satisfied to authorise these electronic surveillance powers against a parliamentarian meant:

*the reference to such rules and protocols is to the relevant Interception of Communication Codes of Practice, and the relevant Official Guidance for the Security and Intelligence Agencies*¹⁸

29. Illustratively, one such Code of Practice, the *UK Code of Practice—Interception of Communications (UK Code of Practice)*, is discussed further below. The Law Council considers it significant that the UK Code of Practice treats ‘confidential personal information and communications between a member of a relevant legislature and another person on constituency business’ as a single category deserving heightened safeguards.¹⁹
30. Furthermore, the UK Code of Practice provides mandatory guidance on the procedures that must be followed by law enforcement authorities when interception of communications and/or the obtaining of secondary data can take place under the

¹⁴ Harold Wilson MP cited in [Caroline Lucas MP & Ors v Security Service & Ors](#) [2015] UKIPTrib IPT/14/79/CH [5].

¹⁵ [Caroline Lucas MP & Ors v Security Service & Ors](#) [2015] UKIPTrib IPT/14/79/CH [7].

¹⁶ *Ibid.*

¹⁷ *Ibid* [33].

¹⁸ *Ibid* [8].

¹⁹ Home Office, [Interception of Communications – Code of Practice](#) (March 2018), 9.42-9.47.

Investigatory Powers Act. The UK Code of Practice states in relation to communications between a member of a relevant legislature and another person on constituency business:

*Where the intention is to acquire confidential personal information, or communications between a member of a relevant legislature (as defined in section 26) and another person on constituency business the reasons should be clearly documented and the necessity and proportionality of doing so should be carefully considered.*²⁰

31. Additionally, the UK Code of Practice also provides for safeguards directed to collateral collection of parliamentary privilege information, for instance where it is 'likely but not intended' that communications between a member of a relevant legislature and a constituent may be collected. In these situations, the UK Code of Practice states consideration should be given to any steps to mitigate the risk of eliciting these communications and if the collateral collection is unavoidable whether special handling arrangements are required within the intercepting authority.²¹
32. The Law Council considers that the provision in the UK's Investigatory Powers Act for binding codes of practice could provide a useful basis for replication in, or adaptation to, Australian legislation. This submission considers specific safeguards in the UK Code of Practice further below.
33. One area of concern in the UK context is whether the Wilson Doctrine encompasses parliamentary metadata. The UK Investigatory Powers Tribunal has found that parliamentary metadata is not within the scope of the Wilson Doctrine.²² The question of whether metadata incidental to the function of Parliament or the work of a committee and elicited under section 178 and 180 of the TIA Act falls within the definition of 'proceedings in Parliament' in section 16(2) of the *Parliamentary Privileges Act 1987* remains unresolved in Australia and is considered further below.

Safeguards on parliamentary communications under the Investigatory Powers Act

34. The Law Council notes without endorsing the UK position in relation to additional safeguards for parliamentary privileged information.
35. The UK Investigatory Powers Act partially incorporates the Wilson Doctrine into legislation by requiring the Prime Minister's approval to authorise interception of communications sent by or intended for parliamentarians.²³
36. In the UK, an equipment interference warrant provides lawful authority to carry out the acquisition of communications stored in or by a telecommunications system. Roughly speaking, this is similar to the function of telecommunications access powers under the TIA Act in Australia. Notably, where an application is made to the Secretary of State for a targeted equipment interference warrant affecting a parliamentarian the Secretary of State may not issue the warrant without the approval of the Prime Minister. Crucially, the additional safeguard applies where the purpose of the warrant is to obtain:
 - communications sent by, or intended for, a person who is a member of a relevant legislature, or

²⁰ Ibid, 101 9.44.

²¹ Ibid.

²² [Caroline Lucas MP & Ors v Security Service & Ors](#) [2015] UKIPTrib IPT/14/79/CH [33].

²³ [Erskine May's Treatise on the law, privileges, proceedings and usage of Parliament](#) (25th edition, 2019), Part 2 Chapter 15, 15.15.

- a member of a relevant legislature's private information.²⁴

37. In the UK, interception and examination with a warrant of the contents of communications is subject to additional safeguards in relation to parliamentarians. For example, section 26 of the Investigatory Powers Act provides, in relation to warrants that would authorise or require the interception of communications sent by, or intended for, a person who is a member of a relevant legislature, the Secretary of State may not issue the warrant without the approval of the Prime Minister.²⁵

Criticism of role of Prime Minister

38. The Law Council notes that the requirement that the Prime Minister approve interception of parliamentary communications was subject to some criticism at the time the Investigatory Powers Act was introduced. For instance, David Davis MP indicated he would prefer removing the role of Prime Minister because of the risk of politicisation.²⁶
39. However, the Joint Committee noted that the risk of politicisation is largely mitigated in the UK context because of the 'double lock' requirement on any warrant for interception which requires a judicial commissioner to review the decision of the Secretary of State to issue a warrant on necessity and proportionality grounds.²⁷ One commentator noted, the requirement for a judicial commissioner to approve a warrant would ensure there was 'no skulduggery in the approval of the warrant and if the judicial commissioner refuses, it is not going to get to the Prime Minister.'²⁸
40. On balance, the UK Joint Committee concluded that the combination of safeguards in the UK system produced the result in an 'effective balance' between 'the need for Parliamentarians to be able to communicate fully and frankly with their constituents and other relevant third parties' and law enforcement policy objectives.²⁹

Broader safeguards for sensitive information

41. The Law Council supports the approach taken in the UK in the Investigatory Powers Act to defining sensitive information, which includes, for example, information subject to legal privilege,³⁰ any information identifying or confirming a source of journalistic information,³¹ and relevant confidential information including communications between Members of Parliament and their constituents.³²
42. Section 2 of the UK Investigatory Powers Act imposes a requirement that the law enforcement authority exercising the surveillance power have regard to, among other factors:
- whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,

²⁴ *Investigatory Powers Act 2016* (UK) s 111(1)(b),

²⁵ *Ibid* s 26.

²⁶ House of Lords and House of Commons, [Joint Committee on the Draft Investigatory Powers Bill](#), Report (11 February 2016) HL Paper 93, HC 651, 136.

²⁷ *Investigatory Powers Act 2016* (UK) s 23.

²⁸ *Ibid*.

²⁹ House of Lords and House of Commons, [Joint Committee on the Draft Investigatory Powers Bill](#), Report (11 February 2016) HL Paper 93, HC 651, 136.

³⁰ *Investigatory Powers Act 2016* (UK) s 2(5)(a).

³¹ *Ibid* s 2(5)(b).

³² *Ibid* s 2(5)(c).

- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.³³

Pre-collection safeguards

43. Given the likelihood that the current electronic surveillance reform process will take additional time to be finalised, the Law Council highlights the need for the use of administratively binding operational protocols and procedures in relation to the collection of privileged information by the NACC and other law enforcement agencies.
44. In this regard, the Law Council notes that the Senate has previously indicated that a protocol should be developed in relation to covert investigation powers and parliamentary privilege.³⁴ By way of analogy, a memorandum in relation to electronic surveillance can draw substantially from existing agreements including the memorandum of understanding on the execution of search warrants in relation to a member of Parliament between the Speaker of the House of Representatives, the President of the Senate, and the Attorney General and the Minister for Home Affairs (**Memo on Search Warrants**);³⁵ and the AFP National Guideline for Execution of Search Warrants where Parliamentary Privilege may be involved (**AFP National Guideline**).³⁶
45. In relation to pre-collection safeguards, the Law Council suggests the Committee consider adopting the following features of the AFP National Guideline, which are also relevant in the context of electronic surveillance:
- appropriate oversight of sensitive investigations—the AFP National Guideline requires the AFP Sensitive Investigation Oversight Board (**SIOB**) to oversee investigations ‘where parliamentary privilege may be involved’;³⁷
 - training of relevant AFP staff on parliamentary privilege—the AFP National Guideline requires online training on parliamentary privilege, the MOU and AFP National Guideline for all AFP members and the lead investigator must ensure all officers involved are training in the requirements of the AFP National Guideline; and
 - mandatory procedures prior to apply for a warrant—

³³ Ibid s 2(2).

³⁴ The President of the Senate said: It was initially hoped new procedures would also be agreed in relation to the exercise of covert powers. However, more work is required to ensure these procedures address the concerns of parliamentarians, particularly in relation to access and use of telecommunications data and the quarantining of material collected covertly. In addition, there are practical issues which the AFP must address to ensure that the agreed procedures do not unduly hamper investigations. Further negotiations regarding the implementation of procedures that ensure covert powers are exercised in a manner which does not intrude on parliamentary privilege will be conducted in the next parliament. Commonwealth, *Parliamentary Debates*, Senate, 23 November 2021, 6512 (Senator Slade Brockman, President of the Senate).

³⁵ Senate Standing Committee of Privileges, Parliament of Australia, [Memorandum of understanding on the execution of search warrants in relation to a member of Parliament between the Speaker of the House of Representatives, the President of the Senate, the Attorney-General and the Minister for Home Affairs](#) (23 November 2021).

³⁶ Australian Federal Police, [National Guideline for Execution of Search Warrants where Parliamentary Privilege may be involved](#) (23 November 2021) (*‘AFP National Guideline’*).

³⁷ Ibid, 2.

- mandatory internal approval from the SIOB before applying for the warrant unless there are circumstances of such seriousness or urgency and/or there is reasonable suspicion that evidence could be destroyed; and
 - the AFP should 'unless a deputy commissioner or the SIOB determines that to do so would affect the integrity of the investigation, contact the member or a senior member of staff prior to executing the warrant.'
46. The Law Council suggests that these existing safeguards in the AFP National Guideline can be improved in the following respects:
- strengthening internal authorisation procedures in relation to telecommunications data powers (discussed further below); and
 - internal approval criteria should require that any electronic surveillance should only be authorised where it is necessary for, and proportionate to, the purposes of an investigation. This is consistent with Recommendation 80 of the Comprehensive Review of the Legal Framework of the National Intelligence Community.
47. The Law Council notes that access to existing telecommunications data under Section 178 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) and access to prospective telecommunications data under Section 180 of the TIA Act may be authorised by an 'authorised officer' and does not require approval from an external authority.
48. The Law Council urges this Committee to consider Recommendation 11 of the PJCIS 2020 Review of the Mandatory Data Retention Regime³⁸ which recommended greater specification of the which officers within a law enforcement agency are designated as 'authorised officers.' By way of illustration, the Committee recommended that section 5AB of the TIA Act be amended with a view to reducing the number of officers of criminal law enforcement agencies who may be designated as 'authorised officers' and the following requirements should be specified:
- only officers or officials who hold a supervisory role in the functional command chain should normally be capable of being designated as 'authorised officers'; although
 - other individuals who hold specific appointments—rather than entire classes of officers or officials—may be capable of being designated as 'authorised officers';
 - in order to authorise an individual to be an authorised officer, the head of an enforcement agency must be satisfied that it is necessary for the individual to be an 'authorised officer' in order for the individual to carry out his or her normal duties;³⁹
49. Additionally, the PJCIS recommended that senior officers considered for nomination as authorized officers should:
- undergo compulsory training in relation to Chapter 4 of the TIA Act;

³⁸ PJCIS, [Review of the Mandatory Data Retention Regime](#) (October 2020).

³⁹ Ibid, Recommendation 11.

- the head of the enforcement agency should be satisfied that the senior officer has the 'requisite experience, knowledge and skills' to exercise powers under Chapter 4 of the TIA Act.⁴⁰

Post collection safeguards

50. The Law Council notes that the AFP National Guideline fails to adequately address in detail post-collection safeguards which protect against misuse of sensitive information when it is collected collaterally. For example, access to information under a stored communication warrant, which may include a person's entire email account, is likely to include a vast trove of information, some of which may be subject to parliamentary privilege.
51. The Law Council notes that the AFP National Guideline requires the case officer to consider restricting access to the case management system and 'such restrictions on access must be used judiciously and reviewed regularly.'⁴¹
52. The Law Council has previously noted that the Investigatory Powers Act contains provisions for the making of binding codes of practice, which set down more detailed procedural requirements in relation to these categories of particularly sensitive information, in the context of specific electronic surveillance techniques.⁴² This aspect of the UK's Investigatory Powers Act could provide a useful basis for replication in, or adaptation to, Australian legislation. The Law Council considers it would aid both compliance and ex post facto oversight, as well as engendering public trust and confidence in the rigour of agencies' protective mechanisms for particularly sensitive forms of information.
53. Illustratively, the UK Code of Practice deals with safeguards in relation to post-collection use of privileged or confidential information including controlling unauthorised disclosure of material, controlling dissemination of material obtained under a warrant, and safeguards in relation to copying, storage and destruction.⁴³
54. The UK Code of Practice also requires details of the arrangements for the handling, retention, use and destruction of such items be included in the warrant application where the purpose of the warrant is to authorise or require the interception of the communications of a member of a relevant legislature.⁴⁴

The scope of proceedings in Parliament

The NBN Co Test

55. The Law Council notes that the Senate Committee of Privileges in 2017, in the first dispute in relation to the 2005 AFP National Guideline, provided a three-part test elaborating on the meaning of 'proceedings in Parliament' in the context of search warrants. This test was an approach derived from the test used by the New South Wales Legislative Council in a case involving the Hon. Peter Breen in 2003–04, and adapted to encompass the definition of 'proceedings in Parliament' as set out in section 16(2) of the Parliamentary Privileges Act 1987 (Cth).⁴⁵

⁴⁰ PJCIS, [Review of the Mandatory Data Retention Regime](#) (October 2020).

⁴¹ AFP National Guideline, 7.

⁴² Law Council of Australia, [Electronic Surveillance Reforms: Submissions on Discussion Paper](#) (18 February 2022) 40.

⁴³ Home Office, [Interception of Communications – Code of Practice](#) (March 2018), 91-97.

⁴⁴ *Ibid*, 31 5.29(o)

⁴⁵ Australia, Senate, Report 163, [Status of material seized under warrant](#), 1 December 2016, para 1.37.

56. The Law Council considers that this definition may serve as a helpful starting point in demarcating the scope of proceedings in Parliament in the context of an electronic surveillance memorandum between Parliament and law enforcement agencies.
- **Step 1:** Were the documents brought into existence in the course of, or for purposes of or incidental to, the transacting of business of a House or a committee?
 - Yes → falls within “proceedings in Parliament”.
 - No → move to Step 2.
 - **Step 2:** Have the documents been subsequently used in the course of, or for purposes of or incidental to, the transacting of the business of a House or a committee?
 - Yes → falls within “proceedings in Parliament”.
 - No → move to Step 3.
 - **Step 3:** Is there any contemporary or contextual evidence that the documents were retained or intended for use in the course of, or for purposes of or incidental to, the transacting of the business of a House or a committee?
 - Yes → falls within “proceedings in Parliament”.
 - No → report that there are documents that fail all three tests.⁴⁶

The scope of ‘proceedings in Parliament’ and metadata

57. The Law Council notes access to telecommunications data under sections 170 and 180 of the TIA Act are subject to internal authorisation within the law enforcement agency. The rationale for the absence of an external authorisation requirement is the distinction drawn between content and non-content information, such as metadata.
58. The basis of this distinction is premised on an assumption that ‘non-content information’ about a communication is, by its nature, necessarily less intrusive to personal privacy than the content of a communication. The Law Council has previously doubted the validity of this assumption stating:

This assumption is dubious in the contemporary environment. Non-content information, particularly when collected in high volumes over an extended period of time, can potentially disclose highly sensitive matters about a person’s activities, movements, associations and personal attributes and affairs. Accordingly, the Law Council cautions that the mere status of information concerning a communication as ‘non-content information’ should not be taken to automatically justify lower levels of authorisation or authorisation thresholds, as compared to those applicable to ‘content information’ in relation to a communication.⁴⁷

⁴⁶ [Senate Committee of Privileges – Search Warrants and the Senate](#), 164th Report (March 2017) 6.

⁴⁷ Law Council of Australia, [Electronic Surveillance Reforms: Submissions on Discussion Paper](#) (18 February 2022) 12.

59. Accordingly, the Law Council agrees with the view expressed by the Senate Privileges Committee that metadata may contain material protected by parliamentary privilege:

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. 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 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.⁴⁸

60. Illustratively, the Law Council notes that parliamentary privilege may apply to telecommunications data where that data reveals the identity of a confidential whistle-blower who has contacted a parliamentarian in relation to matters subject to inquiry by a parliamentary committee.

Mechanism for asserting and resolving disputes as to parliamentary privilege

61. The Law Council acknowledges the three options being considered by the Committee:

***Senator Patterson:** It seems to us that some kind of independent third party needs to make a claim of privilege on behalf of the parliamentarian—a trusted party who wouldn't notify the parliamentarian. The options which we've considered in our public hearings so far are: should it be the Presiding Officers? There are some pros and cons to that. Should it be the clerks of the House or the Senate? There are some pros and cons to that. Or should it be some kind of completely independent third party, such as—as you highlighted in your previous answer—someone who would act as an independent advocate, for example, in relation to journalists when they're subject to these sorts of warrants.*

62. As stated above, given the rationale for parliamentary privilege is so that the legislature maintains exclusive jurisdiction over its own processes, it would undercut this rationale to confer on unelected officials appointed by the executive, such as the Clerks of each House of Parliament, this function. Crucially, a public interest advocate as a statutory office holder will exercise their function in the warrant issuing process subject to the statutory framework.
63. The Law Council also appreciates the risk of politicisation that would arise if presiding officers of Parliament were conferred with this function.
64. The Law Council sets out in further detail below a two-stage approach to the safeguarding of parliamentary privilege information:

⁴⁸ Australia, Senate, Privileges Committee, 168th Report, Parliamentary privilege and the use of intrusive powers, (28 March 2018), 28-29.

- **pre-authorisation safeguard:** the Law Council is supportive of expanding the existing role of public interest advocates for the purposes of Journalist Information Warrants sought under Chapter 4, Part 4-1 of the TIA Act to also include providing public interest submissions in the context of parliamentary privilege—the main purpose of this stage of review is to highlight the potential for parliamentary privilege information to be elicited under the scope of a particular warrant application and to ensure any collection of parliamentary privilege information occurs as a last resort; and
- **post-collection safeguard:** officers appointed by the privileges Committee of the relevant House of Parliament administer a document review process that precisely identifies the documents within the scope of ‘proceedings in Parliament’ applying the NBN Co test outlined above—the main purpose of this stage of review is to assert privilege claims over documents or information. These protections should be bolstered by detailed binding codes of practice that establish guidelines in relation to how investigatory agencies treat parliamentary privilege information discussed above.

65. For the avoidance of doubt, the Law Council notes that it would be impractical to expect a public interest advocate, usually an eminent legal practitioner or former judge, to conduct document review in relation to the vast troves of information that could be elicited under a stored communication warrant in order to assert privilege over particular documents.
66. The Law Council has previously supported an expanded framework to allow a public interest advocate to act as a ‘contradictor’ in the context of electronic surveillance warrant applications more generally.⁴⁹ It is important that issuing authorities have the flexibility to consider whether they would be assisted by such an advocate acting as contradictor in relation to a particular warrant or authorisation request.
67. The Law Council also notes that this Committee has previously recommended the expansion of the public interest advocate regime to cover all overt and covert warrants that relate to a person working in a professional capacity as a journalist or a media organisation, where the warrant is related to the investigation of an unauthorised disclosure of government information, including national security information, or Commonwealth secrecy offence.⁵⁰

The role of a public interest advocate in a warrant application

68. The Law Council considers that the role of the public interest advocate could be to provide independent contradiction of the submissions of the law enforcement agency, such as the NACC, in relation to whether the public interest in granting a surveillance warrant that potentially interferes with parliamentary privilege is outweighed by the public interest in not issuing the warrant.
69. The Law Council suggests that consideration be given to the wider functions of public interest monitors under the *Crime and Corruption Act 2001* (QLD) in relation to some intrusive and covert surveillance powers, for example, covert search

⁴⁹ Law Council of Australia, [Electronic Surveillance Reforms: Submissions on Discussion Paper](#) (18 February 2022) 47-48.

⁵⁰ PJCIS, Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (August 2020), Recommendation 2.

powers⁵¹ and surveillance devices powers.⁵² Section 326 provides a public interest monitor has the following functions

- a) *to monitor compliance by the commission with this Act in relation to matters concerning applications for surveillance warrants and covert search warrants;*
- b) *to appear at any hearing of an application to a Supreme Court judge or a magistrate for a surveillance warrant or covert search warrant to test the validity of the application, and for that purpose at the hearing—*
 - i. *to ask questions of the applicant and to examine or cross-examine any witness; and*
 - ii. *to make submissions on the appropriateness of granting the application; and*
- c) *to gather statistical information about the use and effectiveness of surveillance warrants and covert search warrants;*
- d) *whenever the public interest monitor considers it appropriate—to give to the commission and the parliamentary committee a report on noncompliance by the commission with this Act.*

70. In considering the scope for a public interest advocate under the TIA Act to exercise oversight functions over law enforcement agencies, any potential overlap with the existing oversight function of the Commonwealth Ombudsman should be avoided by clearly demarcating the oversight role of each agency.
71. Additionally, under the *Crime and Corruption Act 2001* (QLD) the applicant must advise the public interest monitor of a surveillance device warrant application under arrangements decided by the monitor⁵³ and the issuing authority must consider any submissions made by a monitor prior to issuing a surveillance warrant.⁵⁴
72. Practically, the operation of the public interest monitor regime in Queensland is characterised by a high degree of consensus building between the monitor and law enforcement applicants to ensure that warrant application conditions are proportionately tailored. For instance, in 2020–21, the Queensland public interest monitor did not oppose any applications for warrants and only opposed one application by the Queensland CCC for the extension of a surveillance device warrant. The public interest monitor observed:

In several cases, prior to the application there was discussion between the PIM and the lawyer representing the QPS or CCC applicant about either the form of the warrant or the sufficiency of the material to be presented in the application hearing. On most occasions where this occurred, the discussion resulted in satisfactory resolution of the issue either by alteration of the form of the draft warrant including amendment of draft warrant conditions or amendment of the application material. If an issue could not be resolved it became the subject of submissions to

⁵¹ *Crime and Corruption Act 2001* (QLD), Part 7.

⁵² *Ibid* Part 6.

⁵³ *Ibid* s 121(7).

⁵⁴ *Ibid* s 123(h).

*the judge or magistrate during the application hearing and the issue was resolved by the judge or magistrate.*⁵⁵

73. In this regard, the Committee might consider the following recommendations:

- inserting a provision in the TIA Act, drawing by way of analogy from section 180H of the TIA Act, that provides, in effect, that an authorised officer must not make an authorisation under section 178 or 180 if the authorised officer ‘knows or reasonably believes’ the target of the surveillance is a parliamentarian;
- requiring external warrant authorisation for surveillance powers likely to interfere with parliamentary privilege, drawing by analogy from the mechanism for obtaining a Journalist Information Warrant under Part 4-1 of the TIA Act;
- providing for an expanded role for the public interest advocate to act as an independent contradictor scrutinising warrant applications likely to interfere with parliamentary privilege similar to the Queensland model; and
- ensuring the Part 4-1 issuing authority is required to consider a public interest test similar to the one in section 180T (2)(b).

74. The Law Council notes its longstanding position that the mere status of information concerning a communication as ‘non-content information’ should not be taken to automatically justify lower levels of authorisation or authorisation thresholds, as compared to those applicable to ‘content information’ in relation to a communication.⁵⁶ Accordingly, the Law Council considers that the power to authorise access to telecommunications data should be limited to judicial officers of superior courts, appointed in their personal capacity.⁵⁷

75. The Law Council notes that the public interest test contained in paragraph 180T(2)(b) of the TIA Act will require some modification in order to be apt to the public interest protected by parliamentary privilege, noting the public interest in parliamentary privilege relates to protecting the freedom of expression necessary for debate in a representative democracy. The Inter-Parliamentary Union and United Nations Office of the High Commissioner state the public interest in parliamentary privilege in terms of protecting the freedom of expression necessary for debate in a representative democracy:

*Parliament can fulfil its role only if its members enjoy the freedom of expression necessary in order to be able to speak out on behalf of constituents. Members of parliament must be free to seek, receive and impart information and ideas without fear of reprisal. They are therefore generally granted a special status, intended to provide them with the requisite independence: they enjoy parliamentary privilege or parliamentary immunities.*⁵⁸

76. Given the focus of parliamentary privilege is to prevent prohibited use rather than disclosure, the public interest advocate must be given sufficient information regarding the likely forensic use to which surveillance information will be put. The

⁵⁵ David Adsett, Public Interest Monitor, [Annual Report 2020-2021](#) (28 October 2021), 4.

⁵⁶ Law Council of Australia, [Electronic Surveillance Reforms: Submissions on Discussion Paper](#) (18 February 2022) 12.

⁵⁷ Ibid 18.

⁵⁸ Inter-Parliamentary Union and United Nations Office of the High Commissioner, [Handbook for Parliamentarians](#) (2016) No. 26, 91.

Western Australian Supreme Court has found that adverse findings by a Corruption Commission may also be an example of prohibited use:

*Prohibited use (that is, the questioning or impeachment of proceedings) includes using evidence of proceedings to support a case that could result in adverse consequences for a member. Such adverse consequences may be findings of criminal or civil liability. It may also include adverse findings as to credibility, character or conduct.*⁵⁹

77. Crucially, at the point of authorisation, there may be some uncertainty as to whether parliamentary privileged information will be collected. In this regard, the proper function of the public interest advocate is to examine the facts of an authorisation request or stored communication warrant, for instance the proposed surveillance method, the target of surveillance, likely third parties whose information may be collaterally collected under the warrant and the duration of surveillance, and then come to an overall judgment on the risk to the public interest protected by parliamentary privilege outlined above.
78. The Law Council encourages the Committee to consider its prior recommendation for statutory codification of mandatory considerations to be addressed by a public interest advocate.⁶⁰ Further, the public interest advocate should be authorised to request information to clarify elements of the warrant application provided by an enforcement agency to enable the case to be built in their submission.⁶¹

Notification of the public interest advocate

79. Given that in the context of electronic surveillance the privilege holder will usually be unaware of the fact of surveillance, it is important for there to be an easily understood point where law enforcement officials are required to notify a public interest advocate in relation to a warrant application likely to infringe parliamentary privilege.
80. Additionally, the Committee might consider imposing an analogous requirement to regulation 12 of the *Telecommunications (Interception and Access) Regulations 2017* which provides that the public interest advocate must be given a proposed journalist information warrant application made by an enforcement agency in order to ensure the public interest advocate receives sufficient notice to provide timely submissions during the authorisation process.
81. If the Committee is inclined to recommend an expanded role for the public interest advocate, the Law Council reiterates its submissions regarding the need for statutory entrenchment of minimum qualifications, consideration of additional powers such as the power to ask the warrant applicant to provide further information and greater public reporting on the role of public interest advocates.

Procedure for asserting privilege in the context of electronic surveillance

82. The Law Council notes that some state legislatures have relevant experience dealing with parliamentary privilege review of information elicited under electronic surveillance in the context of corruption investigations.

⁵⁹ The President of the Legislative Council of Western Australia v Corruption and Crime Commission [No 2] [2021] WASC 223.

⁶⁰ PJCIS, Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (August 2020), Recommendation 2.

⁶¹ Ibid.

83. In 2019, the Western Australian Standing Committee on Procedure and Privileges (**WA Committee on Privileges**) asserted parliamentary privilege in respect of some documents and information arising from the seizure of several electronic devices by the Western Australian Corruption and Crime Commission and Western Australia Police including a parliamentary laptop and back-up hard drives in relation to a prominent corruption investigation.
84. The WA Committee on Privileges found out of a total of 499,174 records obtained under five Corruption and Crime Commission notices to produce subject to parliamentary privilege review, a total of 10,079 records were determined by the WA Committee on Privileges to be subject to parliamentary privilege.⁶²
85. The Law Council notes the procedure adopted by the WA Committee on Privileges may provide more general guidance on a suitable protocol for asserting privilege in relation to information elicited by electronic surveillance:⁶³
- *The use of an initial review team comprised of 11 legally qualified Legislative Council Committee Office staff (each with at least 4 years' post-admission legal work experience). These officers were each appointed as temporary staff of the PPC in order to undertake the audit. These officers all signed additional confidentiality agreements over and above their existing confidentiality agreements as Legislative Council staff.*
 - *Prior to commencing the assessment, the initial review team attended an hour long briefing session on parliamentary privilege conducted by the Clerk and were each provided with a reference folder of all questions asked, speeches given and bills debated by the relevant former Members.*
 - *The review team reviewed the documents in a locked 'Procedure Room', in which each 'reviewer' sat at an individual computer terminal and reviewed documents in electronic form on a monitor in batches of 500 at a time.*
 - *The electronic documents had been locked as read only, and there was no internet access, printing facilities, mobile phones or media storage devices permitted to enter or leave the room during the review. The reviewers worked in teams of a minimum of two in the locked Procedure Room at all times. The Clerk and Deputy Clerk attended at various times during the assessment to answer any queries from the reviewers.*
 - *The initial review team undertook the initial parliamentary privilege assessment of each document, based on the test applied by the New South Wales' Legislative Council for the Breen case and as amended by the Australian Senate Committee of Privileges in its Report 163 into the Conroy case.*
 - *The initial review was conducted over less than nine working days, between Friday, 8 November 2019 and Wednesday, 20 November 2019.*
 - *The reviewers assessed all of the email account data that the CCC had requested from the DPC (that is the subset of documents that fell within the first two Notices to Produce and as reduced by the application of CCC search terms). The reviewers classified each document as being either:*
 - *Not subject to parliamentary privilege;*
 - *Subject to parliamentary privilege; or*

⁶² Standing Committee on Procedure and Privileges, [Progress Report: Supreme Court proceedings and matters of privilege arising in the 40th Parliament](#) (May 2021) 74.

⁶³ Ibid, 60-61.

- *Unsure or requires further information to determine whether it may be subject to parliamentary privilege (such as advice on the intended use of the document by the relevant Member of Parliament).*
- *Documents in the two latter categories were then referred to the Clerk and Deputy Clerk for final individual review and assessment over several days.*
- *An additional assessment of the first category of documents (ie, those assessed to be non-privileged in the initial assessment) was conducted by the Clerk and Deputy Clerk over a further week based on running search terms across the database of:*
 - *various specific email subject headings associated with identified privileged documents (as confirmed by the Clerk and Deputy Clerk); and*
 - *the following key words relating to parliamentary proceedings: speech; motion; notes; research; committee; house; Hansard; petition; amendment; bill; legislation; speak; chamber; briefing; notice; question; privilege; business; PQ; draft, QWN; statement; oppose; Minister; inquiry; support and submission.*

Resolving privilege disputes and the jurisdiction of the Courts

86. In general, the Law Council's long-standing position is that privilege disputes in relation to potentially privileged information should be settled by independent third parties and not by the investigating agency.⁶⁴
87. The Law Council suggests that the Committee give further consideration to the issues that might arise from applying the mechanism for adjudicating disputed privilege claims set out in the Memo on Search Warrants⁶⁵ in the context of electronic surveillance.
88. Clause 5.4 of the AFP National Guideline provides that the member has ten business days from the delivery of the exhibits to the third party to notify the executing officer either that the claim for parliamentary privilege has been abandoned or confirm they intend to formally request 'the appropriate House consider whether the material seized is covered by parliamentary privilege.'⁶⁶ Crucially, the 2021 version of the AFP National Guideline does not contemplate the courts as forum to vindicate claims of parliamentary privilege in relation to compulsory executive powers.
89. The Law Council notes that on one view it is not an appropriate function of the Courts to adjudicate disputes between the legislature and the executive on the existence of privilege in the context of the application of coercive executive powers such as electronic surveillance powers or the power of search. Justice French, as he then was, in *Crane v Gething*⁶⁷ said in respect of the executive power of search:

⁶⁴ Most recently, in relation to the NACC, the Law Council recommended Clause 114 should be redrafted to remove the abrogation of legal professional privilege and to provide for an independent third party, such as a court, to determine claims made in relation to legal professional privilege. Law Council of Australia, National Anti-Corruption Commission Bills 2022 Joint Select Committee on National Anti-Corruption Commission Legislation (14 October 2022) 44.

⁶⁵ Senate Standing Committee of Privileges, Parliament of Australia, [Memorandum of understanding on the execution of search warrants in relation to a member of Parliament between the Speaker of the House of Representatives, the President of the Senate, the Attorney-General and the Minister for Home Affairs](#) (23 November 2021).

⁶⁶ AFP National Guideline, Clause 5.4 item 5.

⁶⁷ *Crane v Gething* [2000] FCA 45.

*The issue of a search warrant is an executive act in aid of an executive investigation. The investigation may lead to the initiation of criminal proceedings. It may clear the person concerned or yield insufficient evidence to justify the initiation of a prosecution. The issue of a search warrant itself does not commence any judicial proceeding. The production of the documents for which privilege was claimed in this case to the Registrar of the ACT Supreme Court and subsequently to the District Registrar of this Court, does not change the character of the seizure. Whether privilege is to be asserted by the Senate must therefore be resolved between the investigating authorities and the parliament.*⁶⁸

90. The Law Council notes that the 2018 version of the AFP National Guideline contemplates the possibility that Courts will decide disputes over privilege claims. For example, the 2018 version stated: 'it is a matter for the Member to determine whether he/she should seek that ruling from a Court or the relevant House.'⁶⁹
91. Referring to the 2018 version of the memorandum of understanding Hall J in the Western Australian Supreme Court identifies that the memorandum of understanding leaves open the Courts as a forum to vindicate a claim of privilege in response to compulsory executive powers:

*The adoption of that procedure in the MOU appears to involve an implicit acceptance that the courts have jurisdiction to determine disputes about the application of parliamentary privilege in the context of compulsory processes. I am unaware of any cases where a ruling has been sought from a court pursuant to this procedure, but it would seem churlish for the courts to deny themselves jurisdiction on the basis that Parliament has exclusive jurisdiction when that exclusive jurisdiction is no longer claimed (if it ever was).*⁷⁰

92. The Law Council has not had the opportunity to consult Constituent Bodies in order to decide a position in respect of this question.
93. The Law Council notes that it is a well-accepted principle of law that Courts have jurisdiction to determine parliamentary privilege questions in two circumstances:
- where a question of parliamentary privilege is raised in a case already before the court, as for example, where a party seeks to rely on something said to done in parliament; and
 - where the court has been asked to review action by parliament to enforce its proceedings, most commonly where parliament has by warrant sought to subject a citizen to restraint by arrest.⁷¹
94. Dixon CJ, stated the overarching principle in the following terms: 'it is for the courts to judge of the existence in either House of Parliament of a privilege, but, given an undoubted privilege, it is for the House to judge of the occasion and of the manner of its exercise.'⁷² In other words, where the existence of parliamentary privilege

⁶⁸ *Ibid*, [45]

⁶⁹ AFP National Guideline for Execution of Search Warrants where Parliamentary Privilege may be involved (15 October 2018) 5.11 4.

⁷⁰ *The President of the Legislative Council of Western Australia v Corruption and Crime Commission* [No 2] [2021] WASC 223, [171].

⁷¹ *Halden v Marks* (1995) 17 WAR 447, 462.

⁷² *The Queen v Richards; Ex Parte Fitzpatrick and Browne* (1995) 92 CLR 157, 162 (Dixon CJ); recently cited in *Leyonhjelm v Hanson-Young* [2021] FCAFC 22, [40] (Rares J) and [358] (Abraham J).

arises as a justiciable issue in proceedings, the court may determine that question without offending the privilege.⁷³

95. In light of this distinction, it is important that a memorandum between the Houses of Parliament and the Attorney General's Department provide a mechanism for impartial third-party adjudication of privilege claim disputes.

⁷³ [Egan v Willis](#) (1998) 195 CLR 424, [5] and [133]; [Amann Aviation Pty Ltd v Commonwealth of Australia](#) (1988) 19 FCR 223, 231-2, [Halden v Marks](#) (1995) 17 WAR 447 considered by White J in [Carrigan v Honourable Senator Michaelia Cash](#) [2016] FCR 1466, [14] and [15].

International Production Orders

96. The Law Council was also asked a question regarding the definitions of issuing authority in relation to authorisation of International Production Orders and a warrant application by a law enforcement officer of the National Anti-Corruption Commission.

97. The Hansard transcript of this exchange reads as follows:

Mr Wilson MP: *If the CLOUD Act was used for the purposes of an investigation under the NACC, I'm just not sure how it's going to work. If the requirements of the CLOUD Act are that warrants are issued by reference to the Security Appeals Division of the AAT and we now have a legislative requirement, apparently, that means that, if you want a warrant for the purposes of the NACC, you have to get one from an eligible judge, I'm not sure whether those two things are possibly going to be inconsistent, or whether the government needs to consider making sure that the enabling legislation, with respect to the CLOUD Act, picks up that difference.*

You could potentially be seeking a warrant through the CLOUD Act arrangements in two separate kinds of circumstances: one that is NACC related and one that is not NACC related. The agreement that we are considering between us and the United States requires that it be the Security Appeals Division (of the Administrative Appeals Tribunal), and yet, for our own domestic purposes under the NACC, it's an eligible judge. I'm not sure if the potential for that inconsistency has been picked up, and I don't know if you've seen anything that might enlighten us on that.⁷⁴

98. The Law Council notes that new items 251A to 251E to the NACC Consequential Bill are addressed to this issue and repeal the definition of 'issuing authority' in Clause 2 of Schedule 1 of the TIA Act in relation to an international production order applied for by the NACC—to mean a person who is a superior Court Judge.

99. The Supplementary Explanatory Memorandum describes the rationale for these amendments in the following terms:

The effect of this amendment would be to provide that only a subset of all issuing authorities under Schedule 1 of the TIA Act are issuing authorities in respect of the NACC—being superior Court Judges. As such, where the NACC has applied for an international production order under clauses 33 or 42 of Schedule 1 of the TIA Act, that order could only be validly issued under clauses 39 or 48 by an issuing authority who is also a superior Court Judge.

The new definition would not affect the ability of other issuing authorities to issue international production orders to agencies other than the NACC.⁷⁵

100. Sub-clause 3(1) of Schedule 1 of the TIA Act defines a 'designated international agreement' to mean an agreement between Australia and a foreign country, and a

⁷⁴ Parliamentary Joint Committee on Intelligence and Security, National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022, [Proof Committee Hansard](#), Wednesday 30 November 2022, 3-4.

⁷⁵ [NACC Supplementary Explanatory Memorandum](#), para. 45 and 46.

copy of the English text of the agreement is set out in the regulations; and the agreement has entered into force for Australia and the foreign country.

101. On 15 December 2021, Australia and the US signed the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (Cloud Act Agreement)*. The Cloud Agreement was tabled in Parliament on 8 February 2022 and is currently being considered by the Joint Standing Committee on Treaties.
102. The Law Council notes that the Cloud Act agreement leaves open the definition of a 'designated authority' under the agreement to the designation of the Minister for Home Affairs. Article 1 of the Cloud Act Agreement defines 'designated authority' to mean 'for Australia, the governmental entity designated by the Minister for Home Affairs.' Article 5(1) provides 'orders subject to this Agreement shall be issued in compliance with the domestic law of the Issuing Party.'
103. As a result, the Law Council does not consider it necessary to specify the different procedures for authorisation in the regulations implementing the Cloud Act Agreement as a 'designated international agreement' under Schedule 1 of the TIA Act.
104. However, the Law Council agrees that retaining these two distinct authorisation procedures for International Production Orders under the same Cloud Act Agreement may result in confusion and unintended consequences.
105. Practically, the Law Council recognises the scope for confusion that may result in the implementation of protocols for authorising International Production Orders under the Cloud Act Agreement within law enforcement agencies. It is also possible that in circumstances where a NACC corruption investigation overlaps with an existing criminal investigation conducted by another law enforcement agency, law enforcement officials will have an incentive to utilise the procedure with the less stringent definition of issuing authority.
106. The Law Council long-standing position is that all electronic surveillance warrants should be issued by judicial officers, to the exclusion of tribunal members. The Law Council considers that a requirement for a judicial officer to authorise the issuance of an electronic surveillance warrant provides a greater degree of independence, both substantive and perceived, in the authorisation process.⁷⁶
107. The Law Council is of the view that the adjudicative skills of judicial officers are particularly well-suited to the factual and legal complexities likely to arise in warrant applications.⁷⁷

⁷⁶ See further, Law Council of Australia, [Electronic Surveillance Reforms: Submissions on Discussion Paper](#) (18 February 2022) 33-34.

⁷⁷ See further, *Grollo v Palmer* [1995] HCA 26, [20].