

25 January 2018

Committee Secretary
Senate Standing Committee of Privileges
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Committee Secretary

UNSW LAW SOCIETY SUBMISSION REGARDING THE INQUIRY INTO
PARLIAMENTARY PRIVILEGE AND THE USE OF INTRUSIVE POWERS

The University of New South Wales Law Society welcomes the opportunity to provide a submission to the Standing Privileges Committee Inquiry into whether existing measures regarding the use of intrusive powers adequately acknowledge and protect parliamentary privilege.

The UNSW Law Society is the representative body for all students in the UNSW Faculty of Law.

Nationally, we are one of the most respected student-run law organisations, attracting sponsorship from prominent national and international firms. Our primary objective is to develop UNSW Law students academically, professionally and personally.

Our enclosed submission reflects the opinions of the students of the UNSW Law Society.

We thank you for considering our submission. Please do not hesitate to contact us should you require any further assistance.

Yours sincerely



Nicholas Parker
Policy Submissions Director



Sophie Berton
Policy Submissions Director

AUTHORS

Policy Submissions Directors – Nicholas Parker, Sophie Berton

Student Contributors – Henry Chen, Seung Chan Rhee

ACKNOWLEDGEMENTS

We acknowledge the support of the following individuals who made this submission possible:

UNSW Faculty of Law Dean - Professor George Williams

UNSW Law Society Co-Presidents - Nikita Harlalka and William Vu

UNSW Law Society Vice-President (Social Justice) – Angad Randhawa

I SUFFICIENCY OF EXISTING PROTOCOLS FOR THE EXECUTION OF SEARCH WARRANTS IN PROTECTING PARLIAMENTARY PRIVILEGE

A *What are the relevant privileges and immunities of members of Parliament?*

Parliamentary privilege is an integral element of the parliamentary system, serving to protect the independence of the legislature. It encompasses the range of powers, privileges, and immunities conferred upon those involved in proceedings in Parliament, and its source lies in s 49 of the Australian Constitution;

‘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.’

The Australian Parliament inherited the privileges of the UK House of Commons, including article 9 of the Bill of Rights: ‘that the freedom of speech or proceedings in Parliament ought not to be impeached or questioned in any court or place outside of Parliament’. The Bill of Rights does not encompass the entirety of parliamentary privilege, which also includes the principle of ‘exclusive cognisance’ – that Parliament should rule its own sphere (for instance, Parliament has the power to issue penalties for contempt).

The only declaration made according to s 49 of the Constitution thus far has been the *Parliamentary Privileges Act 1987* (Cth). This statute did not set out to provide an exhaustive statement of parliamentary privilege,¹ and s 16 only prevents evidence ‘for the purposes of or incidental to business of a House or of a committee’ from being tabled in court. Referring to this statute alone, novel forms of information-gathering by police or intelligence agencies would seem to have no impact on the privileges or immunities of parliamentarians, because the newly-gathered information cannot be tabled in court in any case. And yet they do.

The process of sealing documents retrieved in a search warrant on which a claim of parliamentary privilege is made has no origins in statute. It is a policy decision for which the

¹ *Parliamentary Privileges Act 1987* (Cth) s 5.

reasons were first articulated in 2000, in a submission by counsel representing the President of the Senate in *Crane v Gething*.² The Senate argued that if police were allowed to access the documents, sources of information could be discovered and ‘attacked through other investigations and legal proceedings’ – even if the documents themselves could not be used in court.³ With the agreement of police, a process whereby a neutral third party examines the documents for potential privilege claims has since been enshrined in a 2005 memorandum of understanding. The element of parliamentary privilege with which this inquiry is concerned is both recent and extrajudicial, and thus could be easily altered if policy priorities changed.

In brief, if intrusive powers impact on the privileges or immunities of members of Parliament, it is specifically and entirely related to the limitation of MPs’ freedom of speech, occasioned by the reluctance of constituents to approach them with information. This reluctance would be the product of a climate of fear of reprisals by police or intelligence services, acting on behalf of the executive branch of government.

B *What is the underlying criticism of existing protocols?*

Traditional seizure through the execution of a search warrant contains a clear and necessary element of physical intrusion, and provides a House or its members with a logical opportunity during execution to claim parliamentary privilege. Consequently, search warrant protocols such as the *AFP National Guideline for Execution of Search Warrants Where Parliamentary Privilege May Be Involved* (‘the Protocol’) rely upon promoting a procedure of execution where a member is appropriately afforded opportunity to ‘raise’ a claim of breach of privilege in order to allow review.⁴ Even when a claim of breach of privilege occurs after Australian Federal Police have executed a search warrant such as the Australian Federal Police (AFP) seizure of documents in 2016 at the office of Senator the Hon. Stephen Conroy, the protocol effectively neutralises the potential for contempt through stipulated neutral third-party possession of the contested documents until the House adopted the recommendations of the

² 169 ALR 9.

³ Harry Evans, ‘Parliamentary Privilege and Search Warrants: Will the US Legislate for Australia?’ (Papers on Parliament No 48, Parliamentary Library, Parliament of Australia, 2008).

⁴ Australian Federal Police, *National Guideline for Execution of Search Warrants Where Parliamentary Privilege May Be Involved*, 2005.

Privileges Committee and upheld the claim.⁵ Practical application therefore suggests the effectiveness of existing protocol measures concerning the execution of search warrants relies on implementing a process that leverages the eventual triggering of in-built contingencies that enable the containment of a breach from the point that a House, or the relevant parliamentarian, becomes aware of a problematic intrusion.

The notion that the Protocol is insufficient therefore centres upon either rejecting that existing contingencies are satisfactory to assure Parliamentarians that their freedom of speech in parliamentary proceedings is protected, or that the measures fail to account for contemporary intrusive powers used by the AFP. Satisfactory assurances of a protected right to freedom of speech may arise under the assertion that the Protocol does not offer enough protection to parliamentarians' privilege, or that the process of accessing these protection measures is too disruptive to proceedings. Similarly, the application of the Protocol to contemporary intrusive powers, namely electronic surveillance, may inform an assertion that existing measures do not sufficiently protect a House from all potential intrusions upon privilege.

C *Are these criticisms valid?*

It is our submission that both of these assertions are unfounded. Under s 6 of the Protocol, the process of obtaining and preparing the execution of a warrant is overseen by, at the very least, a Manager in the AFP, and the office of the relevant Department of Public Prosecutions. As to the wording of the terms of reference, search warrants concerning premises of parliamentarians in Parliament House also require notification of the Presiding Officer of the relevant house in s 6.4, and in particular cases the relevant member may even be given specific opportunity to claim privilege under s 6.5 and 6.7.⁶ Beyond these proactive measures, the 2016 Conroy case also validated the merits of the Protocol regarding the safekeeping of documents by a neutral third-party under s 6.11, such that the operative outcome of the warrant's execution was

⁵ Australian Federal Police, *National Guideline for Execution of Search Warrants Where Parliamentary Privilege May Be Involved*, 2005, 4; Standing Committee of Privileges, Senate, *Search Warrants and the Senate* (2017) 7-8 [2.21].

⁶ Australian Federal Police, above n 5, 5.

negated.⁷ The process established under the Protocol therefore provides clear consultation of the legislature in a manner that is respectful to the administration and protection of parliamentary privilege, since improper interference by the AFP can demonstrably be avoided.

Within the broader chapeau of assurances to the protection of freedom of speech afforded to a House, criticism may also arise with regards to the tangible disruption to parliamentary proceedings and functions associated with following the Protocol procedure. In response, our submission emphasises that a distinction ought to be made by the Committee between the execution of search warrants under the Protocol, and the parliamentary process involved with processing a claim of privilege. Potential disruption to essential parliamentary functions, particularly sitting weeks, are alleviated under s 6.6 of the Protocol.⁸ Furthermore, s 6.11 of the Protocol stipulates the opportunity to ‘take copies of any documents before they are secured’.⁹ Not only do these measures demonstrate a sensitivity to parliamentary functions within the Protocol, but its application in the Conroy case revealed that the greater source of delay lay in deliberations as to the merits of the claim by the Senate Privileges Committee; the total disruption of the search warrant’s execution totalled just under 12 hours.¹⁰ No source of unreasonable disruption to members’ parliamentary functions are attributable to the Protocol upon distinguishing its application from parliamentary procedures concerning resolving claims of privilege.

Finally, critics may assert that the execution of warrants pertaining to contemporary intrusive powers do not reliably provide parliamentarians with an equivalent opportunity to raise a claim of privilege in the execution. In counter to such an argument, electronic surveillance, whether by through phone tapping, metadata or any other relevant means exist largely outside the remit of the Protocol, which was formulated with specific consideration to search warrants that involve the physical search of premises.¹¹ For this reason, our submission refers to the wording

⁷ Standing Committee of Privileges, above n 5, 7-8 [2.21].

⁸ Australian Federal Police, above n 5, 5.

⁹ Australian Federal Police, above n 5, 4.

¹⁰ Ashlynn McGhee, ‘AFP Ordered to Return Former Senator Stephen Conroy’s Seized Documents’, ABC (online), 28 March 2017 < <http://www.abc.net.au/news/2017-03-28/afp-ordered-to-return-stephen-conroy-seized-documents/8394590>>.

¹¹ section in guidelines of mou.

of term of reference (a) and recommends that applying the Protocol beyond its intended purview of search warrants unfairly places its measures in a frame of incompatibility and therefore insufficiency. Nonetheless, it is worth noting that further consideration on the implications of intrusive powers on other relevant existing frameworks, as well as the validity of concerns regarding the protection of privilege for forms of surveillance where the intrusion is more covert or on other premises, and whether there are grounds for an expansion of the Protocol lies within the other terms of reference listed for consideration by the Committee.

II IMPLICATIONS OF CONTEMPORARY INTRUSIVE POWERS BY LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ON PARLIAMENTARY PRIVILEGE

A *Do communications with constituents fall within the ambit of parliamentary privilege?*

While constituents bringing information to the attention of members of Parliament according to the might benefit from protections from surveillance, the question is whether parliamentary privilege is the appropriate avenue for these protections. The Senate's submission in *Crane* sidestepped this problem by contending that the information provided by a constituent would directly result in words spoken in Parliament.¹²

The consensus seems to be that communications with constituents are protected only if they result in words being spoken on the floor of Parliament. Records of meetings, or communications resulting in representations to Ministers on behalf of constituents, are not protected.¹³ In *Crane*, French J made the apparently straightforward statement that:

‘The fact that [seized documents] may include names of constituents who have made representations or have had meetings with the Senator and which neither they nor the Senator would want to make public does not of itself raise an issue of parliamentary privilege.’

¹² Harry Evans, above n 3.

¹³ Committee on Standards and Privileges, *Privilege: Hacking of Members' mobile phones*, House of Commons Paper No 14, Session 2010—2011 (2011) 11.

In *R v Chaytor*,¹⁴ Lord Phillips preferred a narrow interpretation, protecting Parliament from judicial and executive interference. Yet his Lordship left the door open for change, saying ‘it is necessary to consider the nature of that connection and whether, if such actions do not enjoy privilege, this is likely to impact adversely on the core or essential business of Parliament.’¹⁵

B How do intrusive powers impact on the privileges and immunities of members of Parliament?

Telecommunications interception, electronic surveillance, and metadata domestic preservation orders operate differently from search warrants because they take place without the subject’s knowledge, precluding MPs from raising issues of parliamentary privilege. But in cases where the MP is unaware of the intrusion, there is no possibility for parliamentary privilege to be claimed at all.

There is a paradox at the core of the intersection of intrusive powers with parliamentary privilege, described by the Committee on Standards and Privileges in the House of Commons as ‘an excursion into the realms of metaphysics’.¹⁶ Unlike personal rights (e.g. privacy), parliamentary privilege is concerned with outcomes. In individual cases, knowledge by MPs and constituents that they are being spied upon is the prerequisite for the limitations on freedom of speech which would occasion a claim of parliamentary privilege. But if the intelligence operation remains undiscovered, then the MP’s behaviour remains undistorted, so there is no relevant privilege to invoke.

However, MPs’ actions might well be influenced by a climate of fear arising from widespread knowledge of the use of intrusive powers by law enforcement. This discussion turns on whether the climate of fear is a reasonable one. In this space, the House of Commons urged caution due to the subjectivity of ‘Members’ impressions of the impact on them’. Discussion of protecting MPs’ sources of information finds a parallel in s 126 of the *Evidence Act 1995* (Cth), which

¹⁴ [2010] UKSC 52.

¹⁵ *R v Chaytor* [2010] UKSC 52, [47].

¹⁶ Committee on Standards and Privileges, above n 13, 15.

protects journalists from having to reveal their sources in court (though this is rebuttable by a public interest test). For example, a person leaking information from the company they work for might fear the loss of their job. But it is difficult to see what reprisals a person providing information to an MP might fear from the police or intelligence agencies, operating impartially.

If such reprisals could be identified, then the climate of fear would be reasonable; intrusive powers would have a discernible impact on freedom of speech in Parliament (and thus privilege); and action should be taken to enable claims of privilege to be made on metadata and intercepted communications. Yet this would only be strictly necessary in cases where communications with constituents resulted in proceedings taking place on the floor of Parliament.

III ADEQUACY OF EXISTING OVERSIGHT AND REPORTING REGIMES ON THE USE OF INTRUSIVE POWERS IN PROTECTING PARLIAMENTARY PRIVILEGE

To assure the integrity of ‘Parliamentary proceedings’, the formulation of any documents for the purposes of the House remain protected processes.¹⁷ Intelligence gathering operations now rely more than ever on newer spectrum ‘intrusive powers’, consisting of metadata retention, telecommunications intercepts and electronic surveillance – collectively known as signals intelligence (SIGINT).¹⁸ Due to secrecy in their use, breaches of privilege cannot be raised by the Member with the Speaker in the traditional fashion.¹⁹ As such, external regimes for law enforcement or intelligence services therefore take precedence in assuring the existence of remedies, if not necessarily preventing possible breaches of privilege.

¹⁷ *Parliamentary Privileges Act 1987* (Cth) s 16(2).

¹⁸ See Australian Signals Directorate, Department of Defence.

¹⁹ Parliament of Australia, *House of Representatives Standing Orders – Chapter 7 Privilege*, 13 September 2016, s 52 – 53.

A Oversight regimes in operation relating to the usage of intrusive powers and technologies.

Several modes of institutional oversight are predominant in the regulation and reportage of conduct amongst law enforcement and intelligence. The scope of the inquiry demands that oversight be examined in consideration of legal accountability and governance.

1 Inspector-General of Intelligence and Security

The IGIS remains the premier mechanism by which accountability in the Australian Intelligence Community ('AIC') is achieved.²⁰ Importantly, the IGIS retains the power to access all reports from the AIC, classified or unclassified, for the purposes of determining compliance.²¹ It should be noted, however, that such oversight does not extend to the Australian Federal Police, among other agencies part of the greater National Intelligence Community ('NIC').²² When it comes to the deployment of intrusive powers, the IGIS has access to all signals intelligence products generated by the community.²³ Until 2011, all domestic surveillance warrants issued to ASIO were checked by the IGIS on a 100% compliance basis, but later switched to a risk based sampling process – as such, many warrants now do not receive compliance checks.²⁴

A finding by the committee that current oversight and reporting regimes on the use of intrusive powers are not sufficient in acknowledging the requirements of parliamentary privilege may find a quantifiable recommendation in amending the practices of the IGIS compliance

²⁰ For reference, the Australian Intelligence Community ('AIC') comprises the Australian Geospatial-Intelligence Organisation (AGO), Australian Secret Intelligence Service (ASIS), Australian Security Intelligence Organisation (ASIO), Australian Signals Directorate (ASD), Defence Intelligence Organisation (DIO) and Office of National Assessments (ONA).

²¹ *Inspector-General of Intelligence and Security Act 1986* (Cth) s 8.

²² Commonwealth of Australia, *2017 Independent Intelligence Review* (Department of Prime Minister and Cabinet, 2017) 21.

²³ Inspector-General of Intelligence and Security, *How IGIS Interacts with the AIC* <<http://www.igis.gov.au/australian-intelligence-community/how-igis-interacts-aic>>

²⁴ Inspector-General of Intelligence and Security, *Annual Report 2011 – 2012* (Commonwealth of Australia, 2012) 24.

evaluation to require the approval of any and all surveillance measures concerning parliamentarians.

2 Office of the Commonwealth Ombudsman

The Commonwealth Ombudsman cooperates closely with the Inspector-General of Intelligence and Security, with a Memorandum of Understanding between the two statutory offices facilitating the processing of administrative complaints against members of the AIC.²⁵ Separately, the Ombudsman inspects the records of the AFP and Australian Crime Commission for compliance in telecommunications interception and surveillance devices.²⁶ Due to the MoU, oversight responsibilities are evenly demarcated between the IGIS for the AIC and the Ombudsman for law enforcement.²⁷

3 Parliamentary Joint Committee on Intelligence and Security

The PJCIS reviews administration of AIC agencies and various matters referred to it by a responsible Minister or Parliament.²⁸ The PJCIS is a direct means by which Members of Parliament can impose the discipline of external scrutiny on intelligence agencies and their conduct independent of the Executive.²⁹ Formerly known as the Parliamentary Committee on ASIO, the *Intelligence Services Amendment Act 2005* (Cth) renamed it to the PJCIS and expanded its remit to encompass all the AIC agencies. Recently, the PJCIS released a report recommending the establishment of independent oversight on metadata retention, and the empowerment of the Ombudsman to do so.³⁰

²⁵ Commonwealth Ombudsman and Inspector-General of Intelligence and Security, *Memorandum of Understanding Between the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security*, 14 December 2015.

²⁶ *Telecommunications (Interception) Act 1979* (Cth); see also *Surveillance Devices Act 2004* (Cth).

²⁷ *Ibid.*

²⁸ *Intelligence Services Act 2001* (Cth) s 29(1).

²⁹ Commonwealth, Royal Commission on Australia's Security and Intelligence Agencies, *General Report* (1984) 25.

³⁰ Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) 264.

It is our submission that the Committee echo this recommendation, due to its positive outcomes relating to involving the legislature at an earlier juncture in the surveillance process as it relates to metadata retention.

D Independent National Security Legislation Monitor

The INSLM, while maintaining a focus on legislative developments, nevertheless reviews to what extent individual rights are contravened by the application of counter-terrorism laws by intelligence bodies, such as those enabling technologically intrusive powers.³¹ In being able to compel answers from security organisations for the purposes of review, INSLM reports examine both legislative impact and their usage by intelligence organisations.

IV WHETHER SPECIFIC PROTOCOLS REGARDING THE RELATIONSHIP BETWEEN INTRUSIVE POWERS AND PARLIAMENTARY PRIVILEGE SHOULD BE ESTABLISHED

A *‘Access by law enforcement or intelligence agencies to information held by parliamentary departments, departments of state (or portfolio agencies) or portfolio agencies in relation to members of Parliament or their staff’*

This term of reference refers to law enforcement or intelligence services accessing information actually held by state agencies about members of Parliament. This could take the form of a search warrant, or a formal request. It does not involve telecommunications interception. Computer hacking, which might provide a means to access the information, does not seem to be the subject of this inquiry.

In our submission, the 2005 Memorandum of Understanding provides adequate protection for parliamentary privilege in the execution of search warrants.

³¹ Commonwealth of Australia, above n 6, 114, para 7.15.

B *‘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’*

Metadata can be used to identify sources. That was the thrust of the 2014 debate on data retention, empowering police to seek warrants to investigate preserved metadata for the purpose of identifying journalists’ sources.

A protocol which would require police or intelligence services to inform MPs (or a neutral third party) of instances where their metadata had been accessed or telecommunications intercepted, allowing them to raise claims of privilege, would be an obvious resolution to these concerns. A level of technical expertise might be necessary in the task of filtering this material, narrowing the pool of candidates.

Yet there exists a broad range of possible responses to issues raised by developments in intrusive technologies, as the agreement between the Speaker of the New Zealand House of Representatives and the New Zealand Security Intelligence Service demonstrates.

C *‘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)’*

The New Zealand agreement presents a perspective strongly opposed to surveillance of MPs in general. Once a person becomes a member of Parliament, NZSIS closes their file on that person and ‘will not generally direct the collection of information against any sitting MP.’³²

³² Privileges Committee, *Question of privilege concerning the agreements for policing, execution of search warrants, and collection and retention of information by the NZSIS*, Interim Report, 2013, <https://www.parliament.nz/resource/en-nz/50DBSCH_SCR5878_1/505f4567d97947012fd02861c7abac2ad5032f86>, 11.

There are two exceptions to this rule. ‘Where a particular MP is suspected of undertaking activities relevant to security’, the Director of NZSIS may personally authorise the collection and ‘provides a confidential briefing to the Speaker of the House about the proposed collection and the reasons for it’.³³ Although NZSIS does not require the Speaker’s approval, MPs targeted by surveillance may, through a separate process, make complaints to the Inspector-General.

The second exception involves information being collected about another person with whom the MP is in contact. This ‘incidental’ information must be attached to the file of that other person, and information about the MP will be destroyed unless it is necessary to provide context.³⁴

This process of restricting the Speaker’s power, by requiring only that they be informed, seems appropriate in light of a case where the Speaker of the South Australian House of Assembly prevented police from executing a search warrant in his own office during an investigation into his business dealings with a convicted criminal.³⁵ The NZ memorandum is consistent with the practice of law enforcement in notifying the Speaker before proceeding with operations on the grounds of Parliament, to avoid miscommunications which could result in charges of contempt of Parliament.³⁶ Although the interference is more subtle in cases of technological intrusion, and thus the possibility of contempt smaller, adherence to the same standards would be an effective means of preserving the freedom of speech of parliamentarians by precluding police intimidation.

Attitudes to parliamentary privilege and intrusive powers in New Zealand have developed in a manner that is strikingly protective of the independence, not just of the legislature, but also of individual MPs. A Memorandum of Understanding like that between the Speaker and NZSIS would present a simple answer to many of the difficulties raised in this submission, by intentionally and dramatically overshooting the mark required to preserve parliamentary privilege.

³³ Privileges Committee, above n 32, 12.

³⁴ *Ibid.*

³⁵ Martin Hinton, ‘Parliamentary privilege and police powers in South Australia’ (2005) 16 *Public Law Review* 99, 99.

³⁶ *Ibid* 115.

V PUBLIC INTEREST CONSIDERATIONS

A Purview of the Committee limited to the execution of warrants

This term of reference may be taken to provide scope for consideration of whether the current framework for the use of intrusive powers in matters that may attract parliamentary privilege perform in the public interest, or the implications for the Committee’s findings upon Public interest immunity. In the case of the latter, it is important to note that public interest immunity pertains to the protection of documents from being produced as evidence upon order of a court ‘if it were injurious to the public interest to do so’, as articulated by Gibbs ACJ in *Sankey v Whitlam*.³⁷ *NSW v Ryan* also found ‘no relevant difference’ between the definition of public interest immunity in common law to its statutory source under s 130 of the *Evidence Act 1995* (Cth).³⁸ Since the interpretation of public interest immunity rests with the courts as per *Crane*, it is our submission that the Committee avoid a strict application of this interpretation of term of reference (e), such that it may bear relevance to the purview of the House under the *Parliamentary Privileges Act 1987* (Cth).³⁹

Chris Wheeler of the Australian Institute of Administrative Law notes that ‘Although the term is a central concept to a democratic system of government, it has never been definitively defined either in legislation or by the courts’.⁴⁰ He went on to cite the 1979 Australian Senate Committee on Legal and Constitutional Affairs Report on the Commonwealth Freedom of Information Bill;

“... ‘public interest’ is a phrase that does not need to be, indeed could not usefully, be defined... . Yet it is a useful concept because it provides a balancing test by which any number of relevant interests may be weighed one against another. ...the relevant

³⁷ *Sankey v Whitlam* (1978) 142 CLR 1.

³⁸ *New South Wales v Ryan* (1998) 101 LGERA 246, in Australian Law Reform Commission, *Uniform Evidence Law*, Report No 102 (2006) [15].

³⁹ Above n 2; Australian Law Reform Commission, n 38.

⁴⁰ Chris Wheeler, ‘The Public Interest, We Know it’s Important, but do we Know What it Means?’ (2006) 48 Australian Institute of Administrative Law Forum 48, 14. Blah (7) in wheeler.

public interest factors may vary from case to case – or in the oft quoted dictum of Lord Hailsham of Marylebone ‘the categories of the public interest are not closed’.⁴¹

As to public considerations in this inquiry, it is our submission that the Committee follow the established position of avoiding any unnecessarily specific or exhaustively-worded particulars that constitute a public interest that may implicate itself as a definition of ‘public interest’ in its findings.

Certainly, the implications of not affording future iterations of this Committee the same freedom and flexibility in applying privilege to contemporary forms of intrusive powers enjoyed currently would paradoxically exacerbate the potential for disruption of parliamentary functions.

⁴¹ Committee on Legal and Constitutional Affairs, Senate, *Report on the Commonwealth Freedom of Information Bill*, (1979).