Law Council
OF AUSTRALIA

Office of the President

3 December 2019

Senator Sarah Hanson-Young
Chair
Senate Environment and Communications References Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

By email: ec.sen@aph.gov.au

Dear Chair

Supplementary Submission: Inquiry into Press Freedom

On 15 November 2019, the Law Council appeared before the Senate Environment and Communications References Committee (**the Committee**) as part of its inquiry into press freedom (**the Inquiry**).

This supplementary submission addresses two issues that were raised by the Committee during the Law Council's appearance. The first question related to whether Australia already has any contested warrant regimes in place, and the second question related to the existence of legislative framework governing the classification of information by federal government agencies.

Contested Warrant Regimes

In the course of the Law Council's evidence before the Committee, Senator Urquhart asked whether Australia has any contested warrant regimes in place.

The Law Council is not aware of any regimes currently operating in Australia that allow the subject of a warrant to contest the application for the issue of the warrant prior to it being issued and executed. However, the legal validity of the warrant can be subsequently challenged in court after it has been issued. Challenges may also be made to the admissibility of evidence obtained as a result of a warrant that was subsequently found to be unlawful.

However, the Law Council is aware of schemes in Australia whereby a Public Interest Advocate (**PIA**) or Public Interest Monitor (**PIM**) is utilised in relation to the process for the issue of certain types of warrants. For example, a procedure involving a PIA is in place in relation to the application for the issue of journalist information warrant under section 180T of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) relating to accessing the telecommunications data of a journalist.

Under this arrangement, subparagraphs 180L(2)(b)(v) and 180T(2)(b)(v) of the TIA Act require the issuing authority to consider whether the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source. In

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

so doing the issuing authority is to have regard to any submissions made by a PIA under section 180X of the TIA Act. As explained in more detail in the Law Council's submission to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**),[1] the PIA assists the issuing authority in its consideration of whether the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source and can effectively 'contest' the issue of the warrant on this limited basis.

The Victorian Parliament also introduced a PIM scheme in 2011. This regime was established, and continues to be governed, by the *Public Interest Monitor Act 2011* (Vic) (**PIM Act**) and the *Public Interest Monitor Regulations 2013* (Vic) (**PIM Regulations**).

In Victoria, there are two PIMs – the Principal PIM and the Deputy PIM. The PIMs must be an Australian lawyer and cannot be a member of Parliament, the Director of Public Prosecutions, the Solicitor for Public Prosecutions or an employee of the Office of Public Prosecutions.[2]

The PIM is conferred functions under the *Major Crimes (Investigative Powers) Act* 2004 (Vic) (**Major Crimes Act**), the *Surveillance Devices Act 1999* (Vic) (**Surveillance Devices Act**), the *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) (**Telecommunications Act**) and the *Terrorism (Community Protection) Act 2003* (Vic) (**Terrorism Community Protection Act**).[3]

The object of the PIM Act is to provide further safeguards for the following 'relevant applications' (as well as their extension, variation, renewal or revocation):[4]

a) coercive powers orders under the Major Crimes Act;[5]

b) telecommunications interception warrants under the Telecommunications Act;[6]

c) surveillance device warrants, retrieval warrants, assistance orders and the approval of emergency authorisations under the Surveillance Devices Act;[7] and

d) covert search warrants, preventative detention orders and prohibited contact orders under the Terrorism Community Protection Act.[8]

[1] Law Council of Australia, Submission No 40.1 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (23 August 2019).
[2] *Public Interest Monitor Act 2011* (Vic) s 8.
[3] Ibid s 1(b).
[4] Ibid s 3.
[5] See Part 1A of the *Major Crimes (Investigative Powers) Act 2004* (Vic) for the role of the PIM. See Part 2 of the *Major Crimes (Investigative Powers) Act 2004* (Vic) for coercive powers orders.
[6] See Part 1A of the *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) for the role of the PIM. This Part applies if an officer of the Police Force or an IBAC Officer intends to apply under the Commonwealth Act for a Part 2-5 warrant or a renewal of a Part 2-5 warrant: s 4. The Part 2-5 warrants are those listed in Division 4 of Part 2-5 of the Telecommunications (Interception and Access) Act 1979 (Cth): Telecommunications (Interception) (State Provisions) Act 1988 (Vic) s 3, definition of 'part 2–5 warrant'.
[7] See Division 1AA of Part 4 of the *Surveillance Devices Act 1999* (Vic) for the role of the PIM. See Subdivision 2 of Division 1 for surveillance device warrants, Subdivision 3 of Division 1 for retrieval warrants, Division 2 for assistance orders and Division 3 for the approval of emergency authorisations.
[8] See Division 1 of Part 1A of the *Terrorism (Community Protection) Act 2003* (Vic) for the role of the PIM. See Part 2 for covert search warrants, Part 2A for preventative detention orders and sections 13L and 13M for prohibited contact orders.

A PIM is entitled to appear at any hearing of a relevant application to test the content and sufficiency of the information relied on and the circumstances of the application. This can involve:

a) asking questions of any person giving information in relation to the application; and

b) making submissions as to the appropriateness of granting the application.[9]

The Law Council notes that while neither the PIM Act nor PIM Regulations include an express public interest assessment provision, the PIM serves an important public interest function and acts as a strong accountability measure on the use and exercise of investigatory powers.[10]

The Administrative Appeals Tribunal hears and determines applications for telecommunications interception warrants. The Supreme Court deals with all other relevant applications, except for tracking devices under the Surveillance Devices Act, which may be heard and determined by the Magistrates' Court.[11]

A PIM scheme has also been operating in Queensland for over twenty years. The PIM and Deputy PIMs are appointed by the Governor in Council.[12] They are conferred functions under the *Police Powers and Responsibilities Act 2000* (Qld) (**Police Powers Act**), the *Crime and Corruption Act 2001* (Qld), the *Terrorism (Preventative Detention) Act 2005* (Qld) and section 104 of the *Criminal Code Act 1995* (Cth).

In the Police Powers Act, the PIM's functions are set out in section 740. The PIM has the function of monitoring a range of matters, including applications by law enforcement authorities for surveillance device warrants, retrieval warrants and covert search warrants and approvals for the use of surveillance devices under emergency authorisations.[13]

When contesting the validity of the application either in the Supreme Court or Magistrates Court, the function of the PIM is to present questions for the applicant to answer and examine or cross-examine any witness and make submissions on the appropriateness of granting the application.[14] The Law Council notes that while in Queensland, as in Victoria, the role of the PIM as set out in section 740 of the Police Powers Act does not include an express public interest assessment function, the PIM acts as an important accountability measure as its functions serve to ensure that investigatory powers are tested in the public interest.

Under both of these schemes once notified, the Advocate or Monitor can provide submissions to the authority issuing the warrant – effectively as a contradictor on behalf of the target of the warrant, albeit limited to framing arguments that it is not in the public interest for the warrant to be issued.

[9] *Public Interest Monitor Act 2011* (Vic) s 14.
[10] Law enforcement agencies required to notify the PIM of a relevant application are Victoria Police, the Australian Criminal Intelligence Commission, the Independent Broad-based Anti-corruption Commission, the Department of Environment Land, Water and Planning, the Department of Economic Development, Jobs Transport and Resources and the Game Management Authority. See Public Interest Monitor Regulations 2013 (Vic) pt 2.
[11] Public Interest Monitor '*Annual Report 2017-2018*' (22 August 2018) 5.
[12] *Crime and Corruption Act 2001* (Qld) s 324; *Police Powers and Responsibilities Act 2000* (Qld) s 740.
[13] *Police Powers and Responsibilities Act 2000* (Qld) ss 740(1)(a), 742(2)(a)-(d).
[14] Ibid s 742(2)(c).

Legislative Framework Governing the Classification of Information

In the course of the evidence, Senator Patrick asked the Law Council a question in relation to the legislative basis for authorising a Commonwealth official to classify a record.

The specific criteria and process for classifying information is set out in the Commonwealth's Protective Security Policy Framework[15] (**PSPF**) which applies to Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013* (Cth) (**PGPA**). One of the core requirements of the PSPF is that each entity must assess the sensitivity and security classification of information holdings and implement operational controls for these information holdings proportional to their value, importance and sensitivity.[16]

The authority to classify information is not set out in any one piece of legislation, however it is noted that Part 2-2 of the PGPA provides duties and authority to accountable authorities of Commonwealth entities.

An 'accountable authority' is defined as the Secretary of a Department of State, the governing body or a person or group of persons prescribed by an Act or the rules to be the accountable authority of the entity.[17] In the case of the Australian Security Intelligence Organisation, for instance, the Director-General of Security is the accountable authority.[18] In the case of the Department of Home Affairs, the Secretary is the accountable authority.

The Law Council notes the evidence provided to the Committee by the Secretary of the Department of Home Affairs on 15 November 2019 that the classification scheme "is enshrined in policy but which in turn is inscribed in the PGPA Act". Mr Pezzullo also noted that the "judgement about the content of a document—which might go to the source, the method, the sensitivity of the information conveyed—is in the hands of and under the PGPA under the authority of each individual agency head, who further have to have regard to their individual legislation".

The effect of the provisions referred to above appears to be that agency heads or 'accountable authorities' have a duty to implement the requirements of the PSPF, however the exact interaction between the governance arrangements enshrined by the PGPA and the PSPF, and the extent to which this interaction gives a Commonwealth official a duty or authority to classify information, is a question best directed to the Attorney-General's Department as the agency with oversight of the PSPF.

We thank you once again for the opportunity to provide this supplementary submission to the Committee.

[15] Australian Attorney-General's Department, *Protective Security Policy Framework* (Policy 8: Sensitive and classified information), <www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx>.
[16] Ibid, B.1.
[17] *Public Governance, Performance and Accountability Act 2013* (Cth), s 12(2).
[18] *Public Governance, Performance and Accountability Rule 2014* (Cth), Sch 1, Section 6.