Law Council
OF AUSTRALIA

Inquiry into the Adequacy of Commonwealth Laws and Frameworks Covering the Disclosure and Reporting of Sensitive and Classified Information

Senate Standing References Committee on Environment and Communications

23 August 2019

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

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote 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 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

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

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

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 the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2019 Executive as at 28 June 2019 are:

- Mr Arthur Moses SC, President
- Ms Pauline Wright, Treasurer
- Mr Tass Liveris, Executive Member
- Dr Jacoba Brasch QC, Executive Member
- Mr Ross Drinnan, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is grateful for the assistance of the Law Society of New South Wales in the preparation of this submission. The Law Council is also grateful to its National Criminal Law Committee and National Human Rights Committee.

Executive Summary

1. The Law Council is grateful for the opportunity to contribute to the Senate Standing References Committee on Environment and Communications' (**Committee**) inquiry into the adequacy of Commonwealth laws and frameworks covering the disclosure and reporting of sensitive and classified information (**Inquiry**).

2. On 7 August 2019, the Law Council provided a submission to the Parliamentary Joint Committee on Intelligence and Security's (**PJCIS**) inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (**PJCIS Inquiry**).[1] Given the focus of the PJCIS Inquiry, the Law Council's submission primarily addressed the adequacy of thresholds and safeguards when seeking to achieve the ideal balance between press freedoms and national security.[2] The Law Council also provided a supplementary submission dated 23 August 2019.[3]

3. As is explained in greater detail below, due to the similarities between the Terms of Refence of the PJCIS Inquiry and the Terms of Reference of the Committee's Inquiry, this submission generally replicates the Law Council's submission to the PJCIS Inquiry and therefore addresses Terms of Reference (a) and (b).

4. The freedom and independence of the press is a cornerstone of democracy.[4] By providing a public forum for debate, it informs citizens through the presentation of current affairs, opinion and analysis.[5] The media is often impacted to a greater extent by the powers granted to law enforcement and intelligence agencies than other types of sectors due to the social and political purposes with which it is charged. Importantly, its part in protecting Australia's rights and freedoms through public interest reporting and protecting and maintaining an open government must not be understated, nor undermined.

5. In order to ensure that the powers of law enforcement and intelligence agencies do not unduly supress public interest reporting through encroachments on the right to freedom of expression and the media, the legitimate public interest in protecting some information from disclosure must be balanced with the need for open government. This requires the powers of law enforcement and intelligence agencies to be proportionate, necessary and contain adequate safeguards.

6. The Law Council notes that there are many secrecy and other offences under Commonwealth law that impact on freedom of the press. However, the Law Council has not had the opportunity to undertake a comprehensive analysis of the myriad of law enforcement and intelligence agency powers that affect press freedom in Australia.

---

[1] Law Council Australia, Submission No 40 to the 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* (7 August 2019) <https://www.lawcouncil.asn.au/resources/submissions/inquiry-into-the-impact-of-the-exercise-of-law-enforcement-and-intelligence-powers-on-the-freedom-of-the-press>.
[2] Parliamentary Joint Committee on Intelligence and Security, 'Terms of Reference', *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Web Page) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/FreedomofthePress/Terms_of_Reference>.
[3] Law Council Australia, Submission No 40.1 to the 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).
[4] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, Un Doc CCPR/C/GC/34 (12 September 2011).
[5] David Rolph et al, *Media Law Cases, Materials and Commentary* (Oxford University Press, 2nd ed, 2015) 3.

7. In the Law Council's view, one of the key areas in Australia's national security law framework that requires urgent addressing is the unauthorised disclosure and secrecy provisions. In 2010, the Australian Law Reform Commission (**ALRC**) published the report *Secrecy Laws and Open Government in Australia* (**the Secrecy Report**).[6] The Law Council has consistently supported the development and amendment of secrecy provisions in a manner consistent with the Secrecy Report.

8. The Secrecy Report provided recommendations which would, in the Law Council's view, properly place secrecy provisions in the context of a system of open and accountable government in a manner consistent with the right to freedom of expression.[7] While the general secrecy provisions introduced into the *Criminal Code Act 1995* (Cth) (**Criminal Code)** in 2018 adopted some of the ALRC's recommendations, namely the differentiation between 'insiders' and 'outsiders', the recommendations of the Secrecy Report relating to the creation of a general secrecy provision that includes an express harm requirement and a public interest exception have not been implemented by the Australian Parliament. Consequently, secrecy provisions have developed in an ad hoc, inconsistent manner, alongside the granting of increased powers to law enforcement and security agencies to intercept and access the data, and encrypted data, of Australian citizens. As a result, there is a stark imbalance between press freedom and the powers of law enforcement and intelligence agencies, in favour of the latter.

9. In light of the fact that the recommendations of the Secrecy Report, published almost ten years ago, have not been fully implemented, as well as developments in the area of national security measures, particularly the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (**EFI Act**), the Law Council considers it timely that a broader, comprehensive review be undertaken of the secrecy provisions that exist within Australia's national security framework.

10. Furthermore, the powers granted to law enforcement and intelligence agencies regarding Australia's interests and national security must be consistent with the implied constitutional right to freedom of political communication, as well as Australia's obligations under international law. The Law Council considers that these rights and freedoms, and the legitimate reasons for their restriction or limitation, should be contained in a domestic, coherent human rights framework, materialising in a federal charter or bill of rights.

Recommendations

11. In relation to the disclosure and public reporting of sensitive and classified information, including the appropriate regime for warrants regarding journalists and media organisations and adequacy of existing legislation, the Law Council recommends that:

    - a public interest test be inserted in the *Crimes Act 1914* (Cth) (**Crimes Act**) so as to make available a public interest defence consistent with the Secrecy Report to persons charged under repealed section 79(6) of the Crimes Act;

    - the general secrecy offences in Division 122 of the Criminal Code should be amended in a manner consistent with the ALRC's Secrecy Report, in particular to include an express harm requirement that for an offence to be committed, the

[6] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 11 March 2010).
[7] Ibid 22.

unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest;

- in consultation and collaboration with relevant stakeholders, the Australian Government should develop and provide guidance material for journalists, media organisations and public agencies on the practicalities of complying with the provisions in Division 122 of the Criminal Code and other federal secrecy provisions;

- the secrecy offences in the *Australian Security and Intelligence Organisation Act 1979* (Cth) (**ASIO Act**), the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) and the *Defence Act 1903* (Cth) (**Defence Act**) should be amended in a manner consistent with the ALRC's Secrecy Report to include an express harm requirement in the case of 'outsiders';

- section 35P of the ASIO Act should provide protection for those outsiders who, in good faith, make public interest disclosures, as well as those who publish such disclosures in the public interest, about Special Intelligence Operations, which at the same time ensures that a disclosure which is genuinely likely to result in serious harm to individuals is not publicly disclosed;

- section 317ZF of the Telecommunications Act should be amended so that a request for disclosure must be authorised unless it would prejudice an investigation, a prosecution or national security, or unless there are operational reasons for the disclosure not being made;

- section 122.5(6) of the Criminal Code should be amended to identify factors that may be considered for the purposes of determining whether the dealing with or holding of information may be in the public interest;

- division 122 of the Criminal Code should be amended so as to place the onus on the prosecution to establish that the disclosure is not in the public interest;

- the definition of 'national security' for espionage, foreign interference and sabotage offences in the Criminal Code as they extend to the country's political or economic relations with another country should be reconsidered;

- the Criminal Code should be amended to introduce a public interest exception to offences of espionage in Division 91 and foreign interference in Subdivision B, Division 92 under the Criminal Code; and

- a good faith defence framed in the terms of repealed section 24F(2) of the Crimes Act should be available for the sabotage offences in Division 82 of the Criminal Code.

- the determination of warrants authorising investigative action of journalists or media organisations, either as the suspect of an offence or as a third party in possession of information relevant to an investigation, would be improved through the:
    - introduction of a legislative public interest test similar to which occurs under the test provided in section 180T of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**);
    - requirement that a 'issuing officer' is a judge of a superior court of record rather than that currently provided in section 3C of the Crimes Act; and

- adoption of a Public Interest Advocate (**PIA**) or Public Interest Monitor (**PIM**) regime that includes appropriate transparency and accountability mechanisms**.**

- any access to retained telecommunications data should be authorised by a warrant issued by an independent court or tribunal;

- section 180H of the TIA Act should be amended to include a paragraph so that a journalist information warrant is required for the authorisation of access to the telecommunications data of any person that may reasonably be believed as being used to identify a journalist's source;

- annual reporting to the Parliament should occur, which includes the:

  - number and identity of PIAs;

  - number of cases where a PIA contested a journalist warrant;

  - number of cases where a PIA attended the hearing of an application for a journalist warrant; and

  - number of journalist warrants that were successfully contested by a PIA;

- the Committee should obtain the advice of former and current PIAs as to whether they are able to effectively perform their roles as defined in the *Telecommunications (Interception and Access) Amendment (Public Interest Advocates and Other Matters) Regulation 2015* (Cth); and

- the TIA Act should be amended so that:

  - a computer access warrant, foreign intelligence warrant or identified persons warrant allow the interception of a communication passing over a telecommunications system only when authorised by the Attorney-General if the Attorney-General is satisfied that the telecommunications service is being or is likely to be used for purposes prejudicial to security; and

  - telecommunications interception under a computer access warrant should be limited to relevant offences under the *Surveillance Devices Act 2004* (Cth) that are serious offences under the TIA Act.

12. Regarding the whistleblower protection regime and protections for public sector employees, the Law Council recommends that:

    - the Australian Government should continue to work towards a comprehensive whistleblower regime and establish a Whistleblower Protection Authority.

13. Further recommendations of the Law Council are that:

    - the Australian Government should work in consultation with civil society towards developing and implementing a mechanism for the protection and enforcement of human rights in accordance with international human rights obligations and jurisprudence through a comprehensive charter or bill of rights; and

    - to build on the ALRC's Secrecy Report and the Independent National Security Legislation Monitor's (**INSLM**) report *Section 35P of the ASIO Act* (**the ASIO Act**

Report), a comprehensive review should be undertaken of the secrecy provisions that exist within Australia's national security framework.

Introduction

14. A fundamental role of the Australian Government is to protect our community, our rights and our freedoms. It is aided by the media, which plays a key role in defending the public interest, holding government to account and scrutinising the exercise of power.

15. The Law Council recognises that the right to freedom of expression is not an absolute right and must be balanced against necessary limitations to maintain public safety and be proportionate to the threat.[8] There must be an appropriate balance between the desirability of open government and the legitimate public interest in protecting some information from disclosure, for reasons including national security, defence, international relations, and privacy considerations.

16. The Law Council acknowledges that it is critical that Australia's law enforcement and security agencies have available to them powers which may, in certain instances, have the effect of curtailing press freedoms in order to allow for the proper investigation of serious offending and the obtaining of intelligence regarding legitimate threats to national security.

17. However, the powers of Australia's law enforcement and intelligence agencies, enacted in laws such as unauthorised disclosure and secrecy legislation, must appropriately balance the need to protect sensitive information with freedom of the press and protections for those making disclosures in the public interest.

18. Australia's democratic values and rule of law and human rights considerations require that official secrecy must be tempered by the public's right to accountable government. Therefore, any secrecy should be proportionately confined to information the disclosure of which would undermine national security and endanger citizens. The Law Council is of the view that Australia's national security measures must:

    - comply with rule of law principles[9] and Australia's international human rights obligations[10];
    - be shown to be necessary to counter the threat posed to the Australian community by foreign actors, and constitute a proportionate response to that threat;
    - contain mechanisms for independent, regular and comprehensive review of both the content and the operation of Australia's national security measures;
    - contain clearly defined key terms to ensure clarity and certainty, to provide limits on the scope of criminal liability and to avoid arbitrary or inconsistent application; and
    - include safeguards to protect against overuse or misuse of executive power.

[8] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(2).
[9] Law Council of Australia, 'Rule of Law Principles' (Policy Statement, 2011).
[10] Law Council of Australia, 'Human Rights and the Legal Profession' (Policy Statement, May 2017).

Background and context

19. In June 2019, search warrants were executed at the Australian Broadcasting Corporation (**ABC**) headquarters in Sydney and at the home of a News Corporation journalist in Canberra. Both 'raids' were conducted by Australian Federal Police (**AFP**) officers who executed search warrants pursuant to the Crimes Act, the former search warrant relating to document on a series of 2017 stories by the ABC relating to 'The Afghan Files',[11] and the latter relating to documents on a story published by the journalist on the alleged overreaching surveillance capabilities of the Australian Signals Directorate.[12]

20. It was stated by the AFP that in both cases, the search warrants related to secrecy offences in Part VI and VII of the Crimes Act.[13] It was reported that the warrant relating to the ABC journalists who produced the stories on The Afghan Files stated that they were suspects in relation to separate offences under subsection 79(6) of the Crimes Act, subsection 73A(2) of the Defence Act and section 132.1 of the Criminal Code.[14] Subsection 79(6) of the Crimes Act contains the offence of the unauthorised disclosure of official secrets. Similar to the ABC journalists, it has been reported that the News Corporation journalist was a suspect in relation to the 'alleged publishing of information classified as an official secret'.[15]

21. In the wake of these events, an inquiry was referred to the PJCIS by the Attorney-General, The Hon Christian Porter MP, on 4 July 2019 pursuant to subparagraph 29(1)(b)(ia) of the *Intelligence Services Act 2001* (Cth)This referral noted that significant public discussion on the importance of press freedoms, particularly in relation to matters of public interest and national security, has occurred in the wake of the recent execution of search warrants at media outlets and private residences of Australian journalists.[16]

22. The referral also noted that the Australian Government is committed to 'ensuring our democracy strikes the right balance between a free press and keeping Australian's safe – two fundamental tenets of our democracy'.[17] Therefore, the Government sought proposals from media organisations and interested bodies which aim to ensure the right balance is struck between a free press and keeping Australians safe.[18]

23. The Terms of Reference for the PJCIS Inquiry required the PJCIS to consider and report on:

    (a) the experiences of journalists and media organisations that have, or could become, subject to the powers of law enforcement or intelligence agencies

---

[11] Elise Worthington and Clare Blume, 'What Do the AFP Raids on the Media Mean For Journalists and their Sources?', *ABC News* (online, 7 June 2019) <https://www.abc.net.au/news/2019-06-06/abc-raids-what-they-tell-us-about-press-freedom/11187364>.
[12] Paul Karp, 'Federal Police Raid Home of News Corp Journalist Annika Smethurst', *The Guardian* (online, 4 June 2019) <https://www.theguardian.com/australia-news/2019/jun/04/federal-police-raid-home-of-news-corp-journalist-annika-smethurst>.
[13] Australian Federal Police, 'AFP Statement on Activity in Canberra and Sydney' (Media Release, 5 June 2019) <https://www.afp.gov.au/news-media/media-releases/afp-statement-activity-canberra-and-sydney>.
[14] John Lyons, AFP Raid on ABC Reveals Investigative Journalism Being Put in Same Category as Criminality', *ABC News* (online, 15 July 2019) <https://www.abc.net.au/news/2019-07-15/abc-raids-australian-federal-police-press-freedom/11309810>.
[15] Australian Federal Police, 'AFP Statement on Search Warrant in Kingston, ACT' (Media Release, 4 June 2019) <https://www.afp.gov.au/news-media/media-releases/afp-statement-search-warrant-kingston-act>.
[16] Letter from Hon Christian Porter MP, Attorney-General, to Chair, Parliamentary Joint Committee on Intelligence and Security, 4 July 2019 <https://www.aph.gov.au/DocumentStore.ashx?id=4ac549d5-117b-46bd-9a8f-011bffb3ddd4>.
[17] Ibid.
[18] Ibid.

performing their functions, and the impact of the exercise of those powers on journalists' work, including informing the public;

(b) the reasons for which journalists and media organisations have, or could become, subject to those powers in the performance of the functions of law enforcement or intelligence agencies;

(c) whether any and if so, what changes could be made to procedures and thresholds for the exercise of those powers in relation to journalists and media organisations to better balance the need for press freedom with the need for law enforcement and intelligence agencies to investigate serious offending and obtain intelligence on security threats;

(d) without limiting the other matters that the Committee may consider, two issues for specific inquiry are:

(i) whether and in what circumstances there could be contested hearings in relation to warrants authorising investigative action in relation to journalists and media organisations; and

(ii) the appropriateness of current thresholds for law enforcement and intelligence agencies to access electronic data on devices used by journalists and media organisations.

22. The Law Council provided a submission to the PJCIS Inquiry on 7 August 2019, which responded primarily to Terms of Reference (c) and (d), namely a focus on the adequacy of thresholds and safeguards when seeking to achieve the ideal balance between press freedoms and national security.[19] The Law Council also provided a supplementary submission dated 23 August 2019.[20]

(a) On 23 July 2019, the Senate referred the Inquiry to the Committee. The Terms of Reference require the Committee consider and report on: the disclosure and public reporting of sensitive and classified information, including the appropriate regime for warrants regarding journalists and media organisations and adequacy of existing legislation;

(b) the whistleblower protection regime and protections for public sector employees;

(c) the adequacy of referral practices of the Australian Government in relation to leaks of sensitive and classified information;

(d) appropriate culture, practice and leadership for Government and senior public employees;

(e) mechanisms to ensure that the Australian Federal Police have sufficient independence to effectively and impartially carry out their investigatory and law enforcement responsibilities in relation to politically sensitive matters; and

[19] Parliamentary Joint Committee on Intelligence and Security, 'Terms of Reference', *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Web Page) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/FreedomofthePress/Terms_of_Reference>.

[20] Law Council Australia, Submission No 40.1 to the 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).

(f) any related matters.

24. As noted above, given the similarities between the Terms of Refence of the PJCIS Inquiry and the Terms of Reference of the Committee's Inquiry, this submission reproduces the Law Council's submission to the PJCIS Inquiry and therefore addresses Terms of Reference (a) and (b).

Australia's human rights obligations

The right to the freedom of expression

25. The Inquiry's Terms of Reference raise a number of significant human rights considerations.

26. Under Article 19(1) of the *International Covenant on Civil and Political Rights* (**ICCPR**), everyone shall have the right to hold opinions without interference.[21] While freedom of opinion under Article 19(1) is absolute, 'the absolute nature of the right ceases once one airs or otherwise manifests one's opinions'.[22]

27. The right to freedom of expression is contained in Article 19(2) of the ICCPR which provides that this right includes:

> *freedom to seek, receive and impact information and ideas of all kinds regardless of frontiers, either orally in writing or in print, in the form of art, or through any other media of his choice.*[23]

28. Article 19(3) of the ICCPR provides that the exercise of the rights provided for in Article 19(2) carries with it 'special duties and responsibilities'.[24] It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

    for respect of the rights or reputations of others; and

    for the protection of national security or of public order (*ordre public*), or of public health or morals.[25]

Freedom of the press and other media

29. In its *General Comment 34: Article 19: Freedoms of Opinion and Expression* (***General Comment 34***), the United Nations Human Rights Committee (**UNHRC**) states in relation to freedom of expression and the media that 'a free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression';[26] and that 'free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential'

---

[21] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(1).
[22] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (3rd ed, 2013) 591.
[23] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(2).
[24] Ibid art 19(3).
[25] Ibid.
[26] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, Un Doc CCPR/C/GC/34 (12 September 2011) [13].

and 'implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion'.[27]

30. According to *General Comment* 34, the ICCPR embraces 'a right whereby the media may receive information on the basis of which it can carry out its function' as well as a corresponding right for 'the public… to receive media output'.[28] An element of the right of freedom of expression is the limited journalistic privilege not to disclose information sources.[29]

31. In particular, the penalisation of a media outlet, publishers or journalists solely for being critical of the government or the political social system espoused by the government can never be considered to be a necessary restriction of freedom of expression.[30]

Restriction for the protection of 'national security'

32. Conformably with international human rights jurisprudence, the Law Council accepts that the protection of national security, inter alia, can justify restrictions on the right to freedom of expression as long as any such restrictions are provided by law and are necessary for the protection of national security.[31]

33. The UNHRC's *General Comment 34* provides that any restrictions must be 'necessary' for a legitimate purpose and must not be 'overbroad'. As to the latter, restrictive measures must:

    (a) conform to the principle of proportionality;

    (b) be appropriate to achieve their protective function;

    (c) be the least intrusive instrument amongst those which might achieve their protective function; and

    (d) be proportionate to the interest to be protected.[32]

34. The justifiable restriction on freedom of expression on the ground of national security is narrowly defined: this ground of restriction is invoked when the political independence or the territorial integrity of the state is at risk.[33] The prohibition of the transmission of 'official secrets' is also a common national security restriction.[34]

35. The UNHRC's *General Comment 34* provides as follows in relation to the withholding of information of legitimate public interest:

> *Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official*

---

[27] Ibid [13].
[28] Ibid [13].
[29] Ibid [45].
[30] Ibid [42].
[31] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(3).
[32] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, Un Doc CCPR/C/GC/34 (12 September 2011) [33]-[34].
[33] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Material and Commentary* (3rd ed, 2013) 612, citing United Nations Commission on Human Rights, *Siracusa Principles of the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 41st sess, Agenda Item 18, UN Doc E/CN.4/1985/4 (28 September 1984) 6.
[34] Ibid 612.

> *secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information.*[35]

36. It has been suggested, on the basis of careful analysis of UNHRC decisions in relation to particular communications, that the UNHRC is reluctant to allow restrictions on free expression on the grounds of national security and public order, at least in the absence of detailed justifications by the state party.[36] Human rights experts have opined that:

> *national security and public order are perhaps the limitations which are most often abused; they are often invoked to protect the elite position of the government of the day, rather than to truly protect the rights of a state's population*.[37]

Absence of a national human rights framework

37. From a broader perspective, the Law Council considers that human rights and fundamental freedoms in Australia should be protected and balanced against other considerations in a coherent legal framework that promotes the understanding that human rights are 'universal, indivisible and interdependent and interrelated'[38], and that any restrictions upon particular rights and freedoms must be in accordance with international human rights jurisprudence. There persists a fundamental disconnect between Australia's obligations at international law, and their translation into Australian domestic legislation.

38. Accordingly, the Law Council continues to advocate for a charter or bill of rights at the federal level.[39]

39. As the Australian Human Rights Commission has commented, a comprehensive rights framework would not always provide simple solutions to the tensions that arise in practice when human rights intersect, such as those between freedoms and security. Sometimes, governments and courts are called upon to make difficult choices that leave parts of a community feeling aggrieved. Nevertheless, a coherent and comprehensive human rights framework would provide a means of reconciling competing human rights claims that focus on *accommodating* the differing needs of the community.[40]

Recommendation:

- **The Australian Government should work in consultation with civil society towards developing and implementing a mechanism for the protection and**

[35] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [30].
[36] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Material and Commentary* (3rd ed, 2013) 612.
[37] Ibid, citing United Nations Commission on Human Rights, *Siracusa Principles of the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 41st sess, Agenda Item 18, UN Doc E/CN.4/1985/4 (28 September 1984) 6.
[38] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).
[39] See Law Council of Australia, 'A Charter: Protecting the Rights of All Australians' (Policy Statement, 29 November 2008).
[40] Australian Human Rights Commission, Submission to the Expert Panel, *Religious Freedom Review* (February 2018).

enforcement of human rights in accordance with international human rights obligations and jurisprudence through a comprehensive charter or bill of rights.

Constitutional protections

40. In the context of the current Inquiry, the Law Council also highlights the effect of the constitutionally implied right to freedom of political communication, and notes that it is not amenable to alteration by legislation. The High Court of Australia has recognised the freedom of political communication as a fundamental common law right necessary for our system of representative government.[41]

41. While this implied freedom may be 'limited to what is necessary for the effective operation of that system of representative and responsible government provided for by the Constitution',[42] it nonetheless will have implications for attempts to stifle media that is inconsistent with Australia's open democratic system of government. However, it is accepted by the Law Council that in the context of laws addressing national security and public order, there may be legitimate countervailing interests which require the imposition of reasonably and proportionate limitations upon freedom of expression.

42. The Law Council notes that it is reported that Nationwide News filed documents in the High Court on 26 June 2019 which seek to strike down the legal basis of the search for two reasons; first, that the warrant issued was invalid due to legal errors, and secondly, that section 79 of the Crimes Act, which underpinned the warrant, is unconstitutional.[43]

43. The ABC has filed a similar challenge albeit in the Federal Court, which seeks a declaration that that the warrant was invalid on several grounds that underline the fundamental importance of investigative journalism and protection of confidential sources. It also challenges the constitutional validity of the warrant on the basis that it impinges on the implied freedom of political communication.[44]

Existing powers of law enforcement and security agencies in relation to journalists

44. The actions of journalists and legitimate whistleblowers which seek to disclose information in the public interest so as to bolster the accountability and transparency of our democracy, are increasingly targeted through the law, such as through secrecy and unauthorised disclosure offences, as well as legislative schemes focused on espionage, sabotage and foreign interference.

---

[41] *Australian Capital Television v Commonwealth* (1992) 177 CLR 106, 139 (Mason CJ). See also *Nationwide News v Wills* (1992) 177 CLR 1, 74 (Brennan J)
[42] *Lange v Australian Broadcasting Corporation* (1997) 145 ALR 96, 112.
[43] Chris Merritt, 'Guarding Against Secrecy', *The Australian* (online, 23 July 2019) <https://www.theaustralian.com.au/inquirer/guarding-against-secrecy/news-story/285727a094a7a30bdd1ae7036d5bb64f>.
[44] *Australian Broadcasting Corporation v Kane* [2019] FCA 1312, [66] (Abraham J); Australian Broadcasting Corporation, 'Notice of a Constitutional Matter under s 78B Judiciary Act 1903', Submission in *Australian Broadcasting Corporation V Martin Kane & Ors*, NSD989/2019, 24 June 2019 <https://www.comcourts.gov.au/file/Federal/P/NSD989/2019/actions>. See also Australian Broadcasting Corporation, 'Statement by David Anderson, ABC Managing Director, on Federal Court Proceedings' (Media Release, 24 June 2019) <http://about.abc.net.au/statements/statement-by-david-anderson-abc-managing-director-on-federal-court-proceedings/>.

45. Broadly, some of the issues that arise in relation to the application of these offences to the activities of journalists and news organisations include:

    (a) the inconsistent manner in which secrecy and unauthorised disclosure provisions have developed in Australia's national security framework;

    (b) the lack of protection for journalists and whistleblowers when national security, intelligence or defence information is disclosed or reported in the public interest; and

    (c) the broad scope of journalistic conduct, which may be innocuous, that can be caught under espionage, sabotage and foreign interference provisions.

Secrecy provisions

Key principles to underpin secrecy offences

46. The ALRC, in its 2015 report, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, examined Australia's secrecy laws in the context of freedom of speech. The ALRC observed:

> *The exposure of state secrets may be seen as falling outside the scope of traditional freedom of speech. However, while the conventions of the Westminster system were once seen to demand official secrecy, secrecy laws may need to be reconsidered in light of principles of open government and accountability—and modern conceptions of the right to freedom of speech.*[45]

47. In a submission to the PJCIS on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth) (**EFI Bill**), the Law Council noted that the ALRC had recommended in its 2015 Report that the general secrecy offences in sections 70 and 79 of the Crimes Act were in need of review as to whether they unjustifiably limit freedom of speech.[46]

48. In response to the subsequent reforms proposed by the EFI Bill, the Law Council submitted that the secrecy provisions contained therein should be amended in a manner which is consistent with the ALRC's Secrecy Report and the INSLM's ASIO Act Report.[47]

49. In the Secrecy Report, the ALRC generally:

- recommended that a general secrecy offence be established for behaviour that harms, is reasonably likely to harm or intended to harm, essential public interests;
- accepted that harm was implicit in any disclosure of information obtained or generated by intelligence agencies;

---

[45] Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws* (Report 129, 2 March 2016) 98 [4.107].
[46] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 56 [184], citing Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws,* 126.
[47] Roger Gyles AO QC, Independent National Security Legislation Monitor, *Section 35P of the ASIO Act* (2016) 18. See Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 12.

- accepted that specific secrecy offences could be justified in this context (the ALRC recommended that many secrecy offences be abolished, and a new general secrecy offence be created);
- recognised in this context a distinction between secrecy offences directed specifically at insiders (who have special duties to maintain secrecy) and those capable of applying to all persons; and
- recommended that secrecy offences capable of applying to persons other than insiders have an express harm requirement.[48]

50. These principles were affirmed by the then INSLM in his analysis of section 35P of the ASIO Act in the ASIO Act Report.[49] In his report, the then INSLM made recommendations regarding the specific secrecy offence relating to special intelligence operations which were subsequently adopted through amendments to the provision.

51. In addition, the ALRC also recommended that:

- the conduct proposed to be regulated by the general secrecy offences should capture 'disclosures of Commonwealth information'; and
- the general secrecy offences carry a maximum penalty 7 years imprisonment.[50]

52. The ALRC's Secrecy Report noted that the general secrecy offence should be limited to 'unauthorised disclosures' that are likely to:

- damage the security, defence or international relations of the Commonwealth;
- prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;
- endanger the life or physical safety of any person; or
- prejudice the protection of public safety.[51]

53. The ALRC further recommended that the general secrecy offence should expressly include, inter alia, a public interest exception.[52] As detailed below, secrecy provisions have not been amended or reformed in a manner consistent with the Secrecy Report nor the ASIO Act Report.

54. The Law Council has not had the opportunity to examine all the federal secrecy laws operating at the federal level. When the ALRC comprehensively canvassed all the federal secrecy provisions, over 500 offences (358 criminal) were identified in 176 pieces of legislation.[53] However, one of the key recent developments which this submission addresses below is the 2018 reforms to general secrecy provisions introduced by the EFI Act. While the EFI Act implemented the ALRC's recommendation to distinguish between 'insiders' and 'outsiders', the remaining principles as outlined by the ALRC's Secrecy Report were not followed in the drafting of the secrecy offences in

[48] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 56.
[49] Ibid.
[50] The Law Council notes that the first INSLM permitted a maximum 10-year penalty in relation section 35P of the ASIO Act: Roger Gyles AO QC, Independent National Security Legislation Monitor, *Section 35P of the ASIO Act* (2016) 24 [46].
[51] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 11 March 2010) 23.
[52] Ibid 241, recommendation 7.1.
[53] Ibid 27 [1.2], 31 [1.20].

Division 122 of the Criminal Code as introduced by the EFI Act, namely the inclusion of an express harm requirement and a public interest exception.[54]

55. With the mapping and analysis of all the federal secrecy exercise occurring ten years ago, and the ongoing expansion of national security legislation, it is submitted that a comprehensive review that builds on the principles of the Secrecy Report and the ASIO Act Report should be undertaken in relation to the secrecy provisions that exist within Australia's national security framework.

Recommendation:

- **To build on the Australian Law Reform Commission's report *Secrecy Laws and Open Government in Australia* and the Independent National Security Legislation Monitor's report *Section 35P of the ASIO Act,* a comprehensive review should be undertaken of the secrecy provisions that exist within Australia's national security framework.**

Repealed official secret provisions

56. While the EFI Act repealed sections 70 and 79 from the Crimes Act in December 2018, the ABC and News Corporation journalists were suspects in relation to the offence under subsection 79(6) because the AFP had commenced both investigations when the provision was still in effect - the ABC investigation in July 2017 and the News Corporation journalist investigation in April 2018.[55] The revised secrecy offences introduced into the Criminal Code by the EFI Act were unable to be relied upon as the alleged conduct occurred before the commencement of those new offences.[56]

57. Prior to 29 December 2018, section 79 of the Crimes Act included several offences that dealt with unauthorised disclosures and the use of official secrets, defence or security information. These provisions were not often used and were difficult to prosecute.[57]

58. Subsection 79(6) made it an offence for a person to receive prohibited information[58] which that person knew, or had reasonable grounds to believe, was communicated to them in contravention of subsection 79(3). A person was in contravention of subsection 79(3) if they communicated to, or permitted access by, a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, a person other than:

    (a) a person to whom he or she is authorised to communicate it; or

[54] Law Council of Australia, Submission No 5.1 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (13 March 2018) 2 [5].
[55] Paul Osborne, 'Key Points in AFP Media Investigations', *The Canberra Times* (online, 6 June 2019) <https://www.canberratimes.com.au/story/6204249/key-points-in-afp-media-investigations/>.
[56] Australian Federal Police, 'AFP Statement on Activity in Canberra and Sydney' (Media Release, 5 June 2019) <https://www.afp.gov.au/news-media/media-releases/afp-statement-activity-canberra-and-sydney>.
[57] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 11 March 2010) 94 [3.118].
[58] A prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information: *Crimes Act 1914* (Cth) ss 79(3), 79(6).

(b) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it.[59]

59. If the relevant fault elements (knowledge or reasonable grounds to believe) of the offence under subsection 79(6) were proven, the only defence available to the defendant was to prove that the communication 'was contrary to his or her desire'.[60] The penalty for this offence was imprisonment for two years.

60. Currently, the journalists being investigated under subsection 79(6) of the Crimes Act do not have recourse to a public interest defence. Furthermore, the *Public Interest Disclosure Act 2013* (Cth) (**PID Act**) (for reasons detailed below) would be unlikely to provide an avenue for authorised disclosure as 'intelligence information' is carved out from 'disclosable information'.

Recommendation:

- **A public interest test be inserted in the *Crimes Act 1914* (Cth) so as to make available a public interest defence consistent with the Australian Law Reform Commission's report *Secrecy Laws and Open Government in Australia* to persons charged under repealed section 79(6) of the *Crimes Act 1914* (Cth).**

New secrecy of information provisions

61. The EFI Act repealed section 79 from the Crimes Act and created new secrecy provisions and defences, including a public interest defence, within the Criminal Code.

62. Division 122 of Part 5.6 of the Criminal Code contains the new general secrecy offences, which replaced Parts VI and VII of the Crimes Act, including:

- offences of inherently harmful information in section 122.1 (penalties ranging from 3-7 years imprisonment depending on relevant fault and physical elements);
- offences of conduct causing harm to Australia's interests in section 122.2 (penalties ranging from 3-7 years imprisonment depending on relevant fault and physical elements);
- aggravated offences for inherently harmful information and conduct causing harm to Australia's interests in section 122.3 (penalties ranging from 5-10 years imprisonment); and
- an offence of unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers in section 122.4 (imprisonment for 2 years).

63. In addition, section 122.4A of the Criminal Code creates offences of communicating or dealing with information where:

- the information has a security classification of secret or top secret;
- the communication of or dealing with the information damages the security or defence of Australia;

[59] *Crimes Act 1914* (Cth) s 79(3).
[60] Ibid.

- interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence; and/or
- harms or prejudices public health or safety.

64. Subsection 122.5(6) of the Criminal Code provides a defence for public interest reporting, including for a person 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media', where at that time the person reasonably believed engaging in that conduct was in the public interest, which is discussed further below.

Express harm requirement

65. The secrecy offences assume that harm is implicit in communication or dealing with certain categories of information. These categories are listed under section 121.1 of the Criminal Code relating to the definitions of 'cause harm to Australia's interests' and 'inherently harmful information'.

66. The problem with such categories is that they extend considerably beyond the essential public interests that the ALRC identified for new general secrecy offences. As noted above, the ALRC recommended that secrecy offences should be 'reserved for behaviours that harms, is reasonably likely to harm or intended to harm essential public interests'.[61]

67. In contrast, the general secrecy offence provisions relate to communications of, or dealings with, information relating to one of the many listed categories in section 121.1 deemed to 'cause harm to Australia's interests' and consisting of 'inherently harmful information'.[62]

68. In its previous advocacy, the Law Council raised its concern that these secrecy provisions may discourage whistleblowers from speaking out publicly.[63] The likely impact is uncertainty as to how information may be communicated or dealt with, without fear of prosecution. The Law Council is concerned that the provisions may have a chilling effect on dissemination of material about security with no relevant connection to the categories of information captured by the provisions.[64]

69. The Law Council considers that the general secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely to cause, harm to an identified essential public interest.[65] Such an element would address concerns about the broad scope of criminal secrecy provisions, which may capture disclosures of information that are innocuous. Where no harm is likely, the ALRC considered that other responses to unauthorised disclosure of Commonwealth information are appropriate, including the imposition of administrative sanctions or the pursuit of contractual or general law remedies.[66] The Law Council further reiterates that,

[61] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 11 March 2010) 23.
[62] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 58 [194].
[63] Ibid 67 [140].
[64] Ibid 59 [199].
[65] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 11 March 2010) 12.
[66] Ibid 249 [8.6].

as noted above, in the Secrecy Report, the ALRC generally accepted that harm was implicit in any disclosure of information obtained or generated by intelligence agencies.[67]

70. As already noted, the Law Council supports updating the general secrecy offences in the Criminal Code in a manner consistent with the ALRC's Secrecy Report.

Recommendation:

- **The general secrecy offences in Division 122 of the *Criminal Code Act 1995* (Cth) should be amended in a manner consistent with the Australian Law Reform Commission's report *Secrecy Laws and Open Government in Australia*, in particular to include an express harm requirement that for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest.**

Addressing ambiguity in the offence

71. The Law Council notes the joint submission to the PJCIS on the EFI Bill from three UN Special Rapporteurs, which stated that they were:

> *particularly concerned that these restrictions will disproportionately chill the work of media outlets and journalists, particularly those focused on reporting or investigating government affairs. The lack of clarity concerning these restrictions, coupled with the extreme penalties, may also create an environment that unduly deters and penalizes whistleblowers and the reporting of government wrongdoing more generally.*[68]

72. In the Law Council's view, subparagraphs 122.4A(1)(d)(ii)-(iv) of the Criminal Code lack precision which leads to the establishment of an unclear threshold for when the offence is triggered. For instance, the Law Council queries:

- the level or degree to which 'the communication of the information' must damage the security or defence of Australia in order to satisfy subparagraph 122.4A(1)(d)(ii);
- the level or degree to which the communication of the information must interfere with, or prejudice, the prevention, detection, investigation, prosecution or punishment of a criminal offence in order to satisfy subparagraph 122.4A(1)(d)(iii); and
- the level or degree, as well as nature, of harm or prejudice to the health or safety of the Australia in order to satisfy subparagraph 122.4A(1)(d)(iv).

73. Furthermore, subsection 122.4A(2) of the Criminal Code creates an offence for 'dealing with' prescribed information. A large and imprecise range of information is potentially captured by the offence provisions, some of it with no likely prejudicial impact on

[67] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 56.

[68] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the Special Rapporteur on the situation of human rights defenders, Submission No 30 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (14 February 2018).

Australia's interests. The below example may assist in demonstrating the breadth of the proposed provisions:

> *A journalist receives an unexpected envelope from a known Commonwealth officer. The envelope contains a copy of a security classified document. While the document has a protected security marking, the journalist reads the document and considers that its contents are innocuous. The journalist shreds the document and no further use is made of it. The mere fact of the journalist receiving the document and possessing it would come within the 'dealing with' 'inherently harmful information' proposed offence provisions. A question may also arise as to whether the destruction of the document in such circumstances would amount to 'concealing' the information which is also captured by the broad definition of 'dealing with'. It is questionable that the proposed defence in subsection 122.5(6) would apply in such circumstances as it may not be considered that they dealt with the information in the public interest or in their capacity as a journalist engaged in fair and accurate reporting.*

74. In the view of the Law Council, the provisions in Division 122 require clarification to ensure that the innocent receipt of information is not captured by the offence provisions. The fault element of intention applies to the communicating or dealing with 'information', which is not necessarily interpreted to mean the information that falls within one of the prescribed categories. The link between the defendant's intention and the harmful behaviours targeted requires further precision. The limited news media defence in subsection 122.5(6) may not be made out as it would be difficult for a defendant to demonstrate there was a reasonable belief in the public interest where they are in receipt of the information but have not had the opportunity to consider its contents.

Recommendation:

- **In consultation and collaboration with relevant stakeholders, the Australian Government should develop and provide guidance material for journalists, media organisations and public agencies on the practicalities of complying with the provisions in Division 122 of the *Criminal Code Act 1995* (Cth) and other federal secrecy provisions.**

Other secrecy provisions

75. The Law Council recognises there is a range of secrecy provisions and unauthorised disclosure offences outside of the EFI Act that impact on freedom of the press, of which the Law Council has not had the opportunity to canvass and analyse.

76. The discussion below provides some examples of secrecy provisions from ASIO Act, the Telecommunications Act and the Defence Act to demonstrate:

- the inconsistencies that exist between each of the secrecy provisions;
- the inconsistency with the Secrecy Report and the ASIO Act Report; and
- the lack of protection for journalists who report, in good faith, certain types of information in the public interest.

ASIO special intelligence operations

77. The *National Security Legislation Amendment Act 2014* (Cth) established a special intelligence operation (**SIO**) scheme within the ASIO Act, based in part on a recommendation by the former INSLM. The SIO scheme permits the Attorney-General

to authorise the carrying out of otherwise illegal activity during ASIO undercover operations.[69] The provisions grant participants of a SIO – including ASIO officers and affiliates – protection from civil and criminal liability.[70] The type of illegal activity that may be permitted is far-ranging and is limited only by extreme criminal activity.[71]

78. In 2015, the former INSLM's ASIO Act Report found that:

> *the impact of section 35P of the ASIO Act on journalists is twofold:*
>
> *(a) It creates uncertainty as to what may be published about the activities of ASIO without fear of prosecution. The so-called chilling effect of that uncertainty is exacerbated because it also applies in relation to disclosures made to editors for the purpose of discussion before publication.*
> *(b) Journalists are prohibited from publishing anywhere at any time any information relating to an SIO, regardless of whether it has any, or any continuing, operational significance and even if it discloses reprehensible conduct by ASIO insiders*.[72]

79. In 2016, the ASIO Act was amended to incorporate some of the recommendations from the INSLM's ASIO Act Report. Section 35P of the ASIO Act was amended from two offences to four: two relating to 'insiders' and two relating to 'outsiders'.

80. The first 'outsiders' offence in subsection 35P(2) applies where a person is reckless as to whether the disclosure will endanger a person's health or safety or compromise the effective conduct of a SIO.

81. The aggravated offence in subsection 35P(2A) requires either knowledge or intention in relation to the harm. This is consistent with the former INSLM's recommendations and reflects the higher standard of conduct that insiders should be held to in relation to their use, handling and disclosure of sensitive information.[73]

82. The former offence attracts a five-year imprisonment term, and the latter a ten-year imprisonment term.[74] These provisions will not apply if the disclosing party believes that the disclosure 'will not endanger the health or safety of any person' or 'will not prejudice the effective conduct of a special intelligence operation'.[75] This amendment is consistent with the INSLM's recommendation.[76]

83. However, in practical terms, these offences may mean that journalists may be disinclined to report on potentially criminal or corrupt conduct rising out of 'ordinary' operations by ASIO out of trepidation that they were aware of a risk that the information may relate to a SIO.[77]

---

[69] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35C(2)(c).
[70] Ibid s 35K.
[71] Section 35K(1)(e) of the Australian Security Intelligence Organisation Act 1979 (Cth) provides that the conduct must not cause death, serious injury, amount to torture or a sexual offence, or cause significant loss of, or serious damage to, property.
[72] Roger Gyles AO QC, Independent National Security Legislation Monitor, *Section 35P of the ASIO Act* (2016).
[73] Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (Cth) [44].
[74] *Australian Security and Intelligence Organisation Act 1979* (Cth) ss 35P(2), 35P(2A).
[75] Ibid s 35P(3A)(c).
[76] Roger Gyles AO QC, Independent National Security Legislation Monitor, *Section 35P of the ASIO Act* (2016) 3.
[77] Law Council of Australia, Submission to the Independent National Security Legislation Monitor, *Inquiry into Section 35P of the ASIO Act* (20 April 2015) 2.

84. In addition, there may also be occasions where a person, including whistleblowers, lawyers, journalists and others, may know or be aware of a substantial risk that information relates to a SIO, but believes it is in the public interest to make the disclosure.

85. There is no public interest defence in the ASIO Act. An additional legislative defence to the SIO offences could provide greater protection for those who, in good faith, make public interest disclosures. Such a defence would need to be framed in a manner which provides sufficient clarity, while still ensuring that information which is genuinely likely to result in serious harm to individuals, is not publicly disclosed.[78]

86. In this context, the Law Council notes that paragraph 80.3(f) of the Criminal Code provides a good faith defence for treason offences where a person publishes in good faith a report or commentary about a matter of public interest.

87. In terms of a disclosure of information relating to a SIO, the Law Council considers that the defence would need to be broader and include situations where a person discloses – not only publishes – about a matter of public interest. This would ensure that individuals who make a legitimate public interest disclosure to a media organisation before the organisation publishes a report or commentary about the matter, will be protected in addition to journalists who may publish the matter. Similar to the good faith defence in paragraph 80.3(f) of the Criminal Code, the court would then be empowered to determine whether the matter was in the public interest.[79]

88. The effect of the provisions is that nothing can be disclosed publicly about a SIO, including if it has been conducted illegally, or an innocent person is killed or tortured. For this reason, it is submitted that section 35P should be amended to ensure that, in extreme circumstances, journalists, lawyers, SIO participants and the public, are permitted to reveal illegal activity, misconduct or corruption that occurs in relation to a SIO.[80]

89. Current or former public officials who make a public interest disclosure under the PID Act would be protected. The PID Act is intended to encourage and facilitate the making of public interest disclosures by public officials and, in some circumstances, provides public officials with protection from liability under secrecy laws.[81]

90. However, disclosures containing 'intelligence information' may only be made internally to authorised persons or to the Inspector-General of Intelligence and Security (**IGIS**).[82] Sections 33 and section 41 of the PID Act exclude 'intelligence information',[83] which

[78] Ibid 4.
[79] Ibid.
[80] Ibid 3.
[81] Law Council of Australia, Submission to Prime Minister and Cabinet, *Public Interest Disclosure Act 2013 (Cth) Review* (28 April 2016) 3.
[82] *Public Interest Disclosure Act 2013* (Cth) ss 26, 33, 41.
[83] 'Intelligence information' is comprehensively defined in section 41 of the PID Act and includes for example: a) information from an intelligence agency; b) information that is about, or that might reveal: i. a source of information referred to in paragraph a); or ii. the technologies or methods used by an intelligence agency to deal with information referred to in paragraph a); or iii. operations that have been, are being, or are proposed to be, undertaken by an intelligence agency; c) information: i. received by a public official from an authority of a foreign government that has functions similar to the functions of an intelligence agency; and ii. that is about a matter communicated by that authority in confidence; d) information from the Defence Department about: i. the collection, reporting, or analysis of operational intelligence; or ii. a program under which a foreign government provides restricted access to technology; e) information: i. that identifies a person as being, or having been, an agent or member of the Australian Secret Intelligence Service; fa) information: i. that identifies a person as an Australian Security Intelligence Organisation (ASIO) employee an ASIO affiliate, a former ASIO employee, or a former ASIO affiliate, f) sensitive law enforcement information.

includes 'sensitive law enforcement information'[84] from external disclosure. Intelligence information may relate to a SIO when it includes information about, or that might reveal 'operations that have been, are being, or are proposed to be, undertaken by an intelligence agency'.[85] As noted by the IGIS in oral evidence before the PJCIS:

> *It is important to notice that neither the Public Interest Disclosure Act nor the Inspector-General's Act allows for unauthorised external disclosure, for example, to a journalist or media organisation, of intelligence information or conduct related to an intelligence agency.*[86]

91. The Law Council acknowledges that, as per the ALRC Secrecy Report, harm can be implicit in any disclosure of information obtained or generated by intelligence agencies (that is, in the case of insiders).

Encryption capability notice requests

92. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**Assistance and Access Act**) amended, among other Acts, the Telecommunications Act in a number of ways. One of which was to introduce a series of 'industry assistance measures' to allow security agencies to request or compel industry to provide technical assistance in the access to, and decryption of, encrypted data. Broadly, this is done through the issuances of notices to industry – technical assistance requests (**TAR**), technical assistance notices (**TAN**) or technical capability notices (**TCN**).

93. The Law Council maintains significant concern about the far-reaching nature of the amendments which were introduced through the Assistance and Access Act. Law enforcement and intelligence agencies have been granted unprecedented powers to exercise intrusive covert powers, accessing messages sent over encrypted messaging software and intercepting communications.

94. Secrecy provisions formed part of these reforms, permitting those issued with notices to disclose information about the existence of such a notice or request in a very limited number of circumstances.[87]

95. Subsections 317ZF(14)–(16) of the Telecommunications Act provide the instances where a designated communications provider and its employees can make authorised disclosures of information relating to a TAR, TAN or TCN. A written request for authorisation to disclose the information must be made to the Director-General of Security or the chief officer of an interception agency in relation to a TAN,[88] or to the Attorney-General in relation to a TCN that has been given by the Attorney-General.[89] If a request for disclosure is authorised, the disclosure must be in accordance with the conditions (if any) specified in the authorisation.

96. The PJCIS recommended in its report on the Telecommunication (Assistance and Access) Bill 2018 (Cth) (**Assistance and Access Bill**) that:

---

[84] *Public Interest Disclosure Act 2013* (Cth) ss 33, 41.
[85] Law Council of Australia, Submission to the Independent National Security Legislation Monitor, Inquiry into Section 35P of the ASIO Act (20 April 2015) 3.
[86] Evidence to Parliamentary Joint Committee Intelligence and Security, Parliament of Australia, Canberra, 14 August 2019, 52 (Margaret Stone, Inspector-General of Intelligence and Security).
[87] *Telecommunications Act 1997* (Cth) ss 317ZF.
[88] Ibid ss 317ZF(14)–(15).
[89] Ibid s 317ZF(16).

> *[it] be amended to allow a provider to request that the Attorney-General approve disclosure of a technical capability. It would be expected that the Attorney-General would agree to such a request except to the extent that doing so would prejudice an investigation or compromise national security. This would complement existing provisions in the Bill that enable a provider to disclose publicly the fact that they were issued a technical capability notice.*[90]

97. While the first part of this recommendation was implemented, as requests are made to the Attorney-General (or the Director-General of Security or chief officer of the interception agency), the second part, relating to the circumstances in which authorisation must be granted, was not.

98. The Law Council has previously noted that these authorised disclosure provisions are not sufficient to ensure that there is a balance between the desirability of open government and the legitimate interest in protecting some information from disclosure, for reasons including national security.[91]

99. For example, if an industry provider to which a notice relates, or one of its employees, was to disclose information about the notice to an individual or body not provided for in the 'authorised disclosure' provisions in section 317ZF, they could be imprisoned for five years,[92] unless a request was made and approved under subsections 317ZG(14)–(16). The Assistance and Access Act grants broad discretionary powers to the Director-General of Security, the chief officer of an interception agency and the Attorney-General, regarding the decision of whether to grant a request for authorised disclosure. The provisions do not provide any indication of the circumstances in which an information disclosure request should or should not be authorised, which is inconsistent with the PJCIS' recommendation stated above.

100. The Law Council is concerned that a request to make an authorised disclosure could be denied on broad, unspecified grounds. The Law Council has previously expressed its support for the PJCIS' recommendation that section 317ZF be amended so that a request for disclosure must be authorised unless it would prejudice an investigation, a prosecution or national security, or unless there are operational reasons for the disclosure not being made.

101. Furthermore, the Law Council notes that the Assistance and Access Act does not provide for a defence to the unauthorised disclosure of information in accordance with the PID Act.

Unlawfully giving or obtaining Defence information

102. As stated above, the ABC journalists involved in the raids which in part led to this Inquiry were identified as suspects in relation to an offence under section 73A(2) of the Defence Act.

103. Under that provision, a person commits an offence if they obtain any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or air force aerodrome or establishment, or to any of the defences of the Commonwealth or any other naval, military or air force information, and that conduct is unlawful.

---

[90] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (December 2018) xiii [2.14].
[91] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunication (Assistance and Access) Act 2018* (Cth) (23 January 2019) 26 [35].
[92] *Telecommunications Act 1997* (Cth) s 317ZF(1).

104. Similar to subsection 122.4A(2) of the Criminal Code, this provision would capture the instance where a journalist simply obtains information relating to defence where it was obtained unlawfully, even if this information was not communicated or published.

Recommendations:

- **The secrecy offences in the *Australian Security and Intelligence Organisation Act 1979* (Cth), the *Telecommunications Act 1997* (Cth) and the *Defence Act 1903* (Cth) should be amended in a manner consistent with the Australian Law Reform Commission's report *Secrecy Laws and Open Government in Australia* to include an express harm requirement in the case of 'outsiders'.**
- **Section 35P of the *Australian Security and Intelligence Organisation Act 1979* (Cth) should provide protection for those outsiders who, in good faith, make public interest disclosures, as well as those who publish such disclosures in the public interest, about Special Intelligence Operations, which at the same time ensures that a disclosure which is genuinely likely to result in serious harm to individuals is not publicly disclosed.**
- **Section 317ZF of the *Telecommunications Act 1997* (Cth) should be amended so that a request for disclosure must be authorised unless it would prejudice an investigation, a prosecution or national security, or unless there are operational reasons for the disclosure not being made.**

Disclosures in the public interest

Journalists' public interest defence

105. As noted above, subsection 122.5(6) of the Criminal Code provides a defence to prosecutions under the secrecy provisions in Division 122 of the Criminal Code for public interest reporting. This defence applies to a person 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media', where at that time the person reasonably believed engaging in that conduct was in the public interest.

106. Generally, the Law Council welcomed the journalistic public interest defence in the EFI Act.[93] However, the Law Council acknowledged that while the journalistic exception is defined more widely than journalism through the reference to 'news media', it remains unclear whether, for example, an individual blogger would fall within this definition.[94]

107. Moreover, the Law Council has previously submitted that the term 'public interest' is not defined, although subsection 122.5(7) sets out several matters that are not in the public interest, such as the dealing or holding of information that would publish the identity of an intelligence officer, contravene witness protection laws or 'will or is likely to harm or prejudice the health or safety of the public or a section of the public'.

108. The term 'public interest' does not set out factors that favour allowing the dealing with or holding of information in the 'public interest'. The determination therefore relies

[93] Law Council of Australia, Submission No 5.1 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (13 March 2018) 5 [30].
[94] Ibid.

on judicial interpretation under the common law. In the absence of factors or criteria which suggests what may amount to the public interest, there may be uncertainty for journalists in the likely application of the defence provision. There remains a concern that this may have a chilling effect on fair and accurate reporting.[95]

109. The journalist defence appears to be set out in an objective way so that a court will be required to make the decision as to whether the conduct was in the public interest rather than the defendant reasonably believed that the dealing with or holding of information was in the public interest.[96]

110. Generally, a public interest test would require a balancing of factors for and against the dealing with or holding of information, with the exceptions which would be contrary to the public interest for identified reasons. The terms of the provision are generally regarded as a total expression of the content of the public interest,[97] although the defence in subsection 122.5(6) is drafted in a broad way which may allow for scope to evaluate or balance competing interests. The question of public interest needs to be assessed having regard to matters specific to the document or information in issue.[98] The fact that a section of the public may be interested in an activity does not necessarily establish a public interest.[99] A disclosure that is contrary to the interests of the government does not necessarily mean it will be contrary to the public interest.[100]

111. Matters that have previously been found to be in the public interest favouring disclosure include, for example, the interest in:

(a) shedding light on whether an agency has acted in accordance with the law or whether it is soundly administered;[101] and

(b) finding out about current decision-making at a stage where it is still possible to contribute to that process and the interest in discovering what has transpired.[102]

112. Under equitable principles, mere exposure to public discussion, review and criticism of government action is not necessarily enough to show a detriment to the government.[103] A government's claim to confidentiality may be measured by injury to the public interest where a disclosure would prejudice the security, relations with foreign countries or the ordinary business of government.[104] The degree of embarrassment to, for example, Australia's foreign relations may also be relevant to the assessment.[105]

---

[95] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 67 [243].
[96] Ibid [244].
[97] *Re Edelsten and Australian Federal Police* (1985) 9 ALN N65; *Re O'Donovan and Attorney-General's Department* (1985) 8 ALD 528; *Ryder v Booth* [1985] VR 869.
[98] *Re Chapman and Minister for Aboriginal and Torres Strait Islander Affairs* (1996) 43 ALD 139.
[99] *Re Public Interest Advocacy Centre and Community Services and Health (No 2)* (1991) 23 ALD 714; *Re Angel and Department of Arts, Heritage & Environment* (1985) 9 ALD 113.
[100] See *Re Bartlett and Department of the Prime Minister and Cabinet* (1987) 12 ALD 659. In *Fisse v Secretary, Dept of the Treasury* (2008) 172 FCR 513, Flick J expressed some reservation as to the conclusion reached in *Re Bartlett and Department of the Prime Minister and Cabinet.*
[101] *Re Lianos and Secretary, Department of Social Security* (1985) 7 ALD 475, 500-1 (Hall DP); *Re Downie* (1985) 8 ALD 496; *Re Birrell and Department of Premier & Cabinet (Nos 1 & 2)* (1986) 1 VAR 230, 240-1.
[102] *Re Lianos and Secretary, Department of Social Security (No 2)* (1985) 9 ALD 43, 49 (Hall DP); *Re Young and State Insurance Office* (1986) 1 VAR 267.
[103] *Commonwealth v John Fairfax & Sons Ltd* ('*Defence Papers case*') [1980] HCA 44, [29] (Mason J).
[104] Ibid
[105] Ibid [37].

113. The publication of confidential information may be found to be in the public interest where it is to protect the community from destruction, damage or harm, or it discloses things done in breach of national security or in breach of the law (including fraud).[106] Public interest may also include preventing unfair commercial advantage, breaches of privacy or prejudice to the orderly administration of the executive government.[107]

114. The Law Council recommended in its submission on the EFI Bill that it should include a public interest disclosure defence to the secrecy provisions where the disclosure would, on balance, be in the public interest. Such reform should non-exhaustively identify some factors that may be considered for the purposes of determining whether the dealing with or holding of information may be in the public interest for the purpose of the journalist defence. Such factors may include for example:

- promoting open discussion of public affairs, enhancing government accountability or contributing to positive and informed debate on issues of public importance;
- informing the public about the policies and practices of agencies in dealing with members of the public;
- ensuring effective oversight of the expenditure of public funds;
- the information is personal information of the person to whom it is to be disclosed; and
- revealing or substantiating that an agency (or a member of an agency) has engaged in misconduct or negligent, improper or unlawful conduct.

Recommendation:

- **Section 122.5(6) of the *Criminal Code Act 1995* (Cth) should be amended to identify factors that may be considered for the purposes of determining whether the dealing with or holding of information may be in the public interest.**

115. In addition, as section 122.5(6) is framed in such a way as to provide a defence for journalists prosecuted under Division 122 of the Criminal Code, which may place the burden on journalists to prove the elements of the section 122.5(6) defence beyond reasonable doubt. Whereas, if Division 122 contained a specific exemption of public interest reporting by the press, the burden would fall on the prosecution to establish that the exception does not apply in a particular case.

116. The Law Council notes that it is ordinarily the role of the prosecution to prove the elements of an offence. Provisions that reverse the burden of proof and require a defendant to disprove, or raise evidence to disprove, one or more elements of an offence, interferes with this common law right.

117. While in this provision the defendant bears an evidential burden rather than a legal burden, the Law Council is of the view that it is inappropriate to place the burden of proof on the defendant and rather this should remain the responsibility of the prosecution.

118. The Secrecy Report recommended that the general secrecy offence should expressly include an *exception* which applies where the disclosure is in accordance with

[106] Ibid [57].
[107] *Deacon v Australian Capital Territory* [2001] ACTSC 8, [87].

an authorisation given by an agency head or minister that the disclosure would, on balance, be in the public interest.[108]

Recommendation:

- **Division 122 of the *Criminal Code Act 1995* (Cth) should be amended so as to place the onus on the prosecution to establish that the disclosure is not in the public interest.**

Whistleblower protection authority

119. In 2017 the Parliamentary Joint Committee on Corporations and Financial Services inquired into and reported on whistleblower protections in the corporate, public and not-for-profit sectors (**Whistleblower Protections Report**).[109]

120. The Law Council has consistently expressed strong support for the establishment of a comprehensive whistleblower regime as identified in the Whistleblower Protections Report, including:

- the creation of a single Whistleblower Protection Act covering all areas of Commonwealth regulation;
- access to non-judicial remedies (e.g. through the Fair Work Commission under the PID Act);
- an agency empowered to implement the regime such as a whistleblower protection authority; and
- appropriate resourcing for effective implementation.

121. One of the Committee's main recommendations was the establishment of a Whistleblower Protection Authority, to be housed within a single body or an existing body, that can support whistleblowers, assess and prioritise the treatment of whistleblowing allegations, conduct investigations of reprisals, and oversight the implementation of the whistleblower regime for both the public and private sectors.[110] The Law Council strongly supports the establishment of such a body.

Recommendation:

- **The Australian Government should continue to work towards a comprehensive whistleblower regime and establish a Whistleblower Protection Authority.**

Espionage, sabotage and foreign interference

Scope of the definition of 'national security'

122. The Law Council has concerns that Australian businesses, advocacy groups and journalists may be caught by the espionage offences in Division 91, sabotage offences

[108] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 11 March 2010) recommendation 7.1(b).
[109] Parliamentary Joint Committee on Corporations and Financial Services, Parliament of Australia, *Whistleblower Protections* (Report, September 2017).
[110] Ibid ch 12.

in Division 82 and foreign interference offences in Division 92 of the Criminal Code for innocuous conduct that is undertaken as a matter of course or in the public interest due to the breadth of the definition of 'national security' that applies to these offences.[111]

123. The espionage, sabotage and foreign interference offences rely on the definition of 'national security',[112] which includes 'the country's political, military or economic relations with another country or other countries'.[113] In all three submissions made by the Law Council to the PJCIS on the EFI Bill, concern regarding the definition of 'national security' was raised.[114]

124. For example, section 91.1 of the Criminal Code creates the espionage offence of dealing with information concerning national security which is or will be made available to a foreign principal with either intention or recklessness as to national security (carrying a penalty of life for intentional conduct or 25 years imprisonment for reckless conduct). The espionage offences in Division 91, with the economic and political elements of the definition of national security, would seem to cover the sort of information that well-informed journalists, academics and consultants of all sorts routinely have access to.[115] Whistleblowers or journalists revealing, for example, harmful conditions in detention centres, misconduct or corruption or reporting on politics or economics, could potentially be captured by the espionage offences in Division 91.[116]

125. Division 92 of Part 5.3 of the Criminal Code contains foreign interference provisions, which apply when a person's conduct is covert or deceptive, involves threats or menaces, or does not disclose the fact that the conduct is undertaken on behalf of a foreign principal.[117] When introduced through the EFI Act, the Law Council did not support the foreign interference provisions, partly because of the definitional issues that arise with 'national security'.[118] The same definitional issue arises in relation to subdivision B of Division 82, which contains the offences of sabotage as to 'national security'.[119]

126. With regards to the foreign interference offences in Division 92, Subdivision B, the Law Council maintains its concern about the possibility of investigative journalists or ordinary citizens being captured. For example, an investigative journalist or a citizen exercising the freedom of expression may engage in 'covert' conduct to influence the exercise of an Australian democratic or political right in collaboration with a person acting on behalf of a foreign principal.[120]

127. The Explanatory Memorandum to the EFI Bill explains that:

> *The reference to 'covert' is intended to cover any conduct that is hidden or secret, or lacking transparency. For example, conduct may be covert if a person takes steps to conceal their communications with the foreign principal, such as*

[111] Ibid 45 [137].
[112] *Criminal Code Act 1995* (Cth) s 90.4(1).
[113] Ibid s 90.4(1)(e).
[114] Law Council of Australia, Submission No 5.2 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (21 March 2018) 2.
[115] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 47 [144].
[116] Ibid [146].
[117] Ibid 50 [152].
[118] Ibid [154].
[119] Ibid 34 [85]-[89].
[120] Ibid 50 [155].

deliberately moving onto encrypted communication platforms when dealing with the foreign principal, meeting in a concealed location, communicating by coded messages, or leaving communications in a concealed location for collection by the foreign principal. Conduct may also be covert if the defendant copies documents or listens into private conversations without the targeted person's knowledge or consent, and then passes that information to a foreign principal.[121]

128. In its report *Keeping Secrets: The Protection of Classified and Security Sensitive Information,* the ALRC did not recommend that 'national security' be defined to include political and economic relations with another country for the purposes of espionage, sabotage and foreign interference offences.[122] In the absence of additional safeguards which were also recommended by the ALRC, such as a requirement of harm and application only to all Commonwealth officers, where a broad concept of 'national security' is employed, the Law Council remains concerned about the inappropriate reference to political and economic relations with another country.[123]

Defences

129. Charges of espionage, foreign interference and sabotage cannot be defended with a public interest or good faith defence. In the absence of any defence under the Criminal Code to a prosecution under Division 91 that the disclosure of information at issue is in the public interest, the offence provisions could have a significant chilling effect on the freedom of media outlets to publish information relating to Australia's national security.[124]

130. Similarly, it is not clear that the defence in paragraph 91.4(1)(a) (in accordance with a law of the Commonwealth) would be available in these kinds of situations if the defendant is unable to point to a specific law of the Commonwealth that they acted in accordance with (noting the proposed evidential burden of proof on the defendant).[125] Unlike the secrecy provisions in Division 122, there are no defences to a prosecution under Division 91 for journalists reporting or for individuals discussing domestic or international politics or economics.[126]

131. While circumstances of investigative journalism on behalf of or in collaboration with a foreign principal or person acting on behalf of a foreign principal may in practice be rare, the Law Council considers that there should be a defence available for persons acting in the public interest for the foreign interference offences in Division 92, Subdivision B.

132. Lastly, before the reforms introduced by the EFI Act, subsection 24F(2) of the Crimes Act provided a 'good faith' defence to a charge of sabotage, which was directed at protecting political communication. However, this defence was replaced and replaced with a fair more limited 'good faith' defence.[127]

---

[121] Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth), [9].
[122] Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98, June 2004).
[123] Law Council of Australia, Submission No 5.2 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (21 March 2018) 2.
[124] Ibid Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Security and Intelligence, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 47 [146].
[125] Ibid [145].
[126] Ibid 48 [149].
[127] Ibid 36-7 [97]-[102].

Recommendations:

- **The definition of 'national security' for espionage, foreign interference and sabotage offences in the *Criminal Code Act 1995* (Cth) as they extend to the country's political or economic relations with another country should be reconsidered.**
- **The *Criminal Code Act 1995* (Cth) should be amended to introduce a public interest exception to offences of espionage in Division 91 and foreign interference in Subdivision B, Division 92 under the Criminal Code.**
- **A good faith defence framed in the terms of repealed section 24F(2) of the *Crimes Act 1914* (Cth) should be available for the sabotage offences in Division 82 of the Criminal Code.**

Contested hearings for warrants concerning journalists

133. The Terms of Reference refer to whether and in what circumstances there could be contested hearings in relation to warrants authorising investigative action in relation to journalists and media organisations.

134. Section 3E of the Crimes Act permits an 'issuing officer' to issue a warrant to search premises if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidentiary material at the premises. An 'issuing officer' is a magistrate, a justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest, as the case may be.[128]

135. The AFP obtained the search warrant for the ABC headquarters from a registrar of the New South Wales Local Court and the search warrant for the home of the News Corporation from a Magistrate of the Australian Capital Territory.[129]

136. Media organisations and other public interest bodies have called for a legislated requirement that all applications for the issue of search warrants relating to journalistic activities must be able to be contested by the media organisation to which the warrant relates. The Law Society of New South Wales submits that a court should examine the proportionality and reasonableness of any warrant application in a judicial hearing, as this would ensure that a requirement to provide reasons and justiciability should the warrant be granted.

137. Furthermore, it has been proposed that a requirement be introduced so that the Attorney-General's approval is sought for all warrant applications regarding journalists and media organisations.[130] The Law Council notes that there is some precedent for this, for example, the ASIO Act provides that the Director-General of Security is to seek the Attorney-General's consent to the issuance of a questioning warrant.[131]

---

[128] *Crimes Act 1914* (Cth) s 3C definition of 'issuing officer'.
[129] Bevan Shields, 'AFP Opens Door to Prosecuting Journalists After Raids, Denies Government Interference', *The Sydney Morning Herald* (online, 6 June 2019) <https://www.smh.com.au/politics/federal/afp-opens-door-to-prosecuting-journalists-after-raids-denies-government-interference-20190606-p51v77.html>.
[130] Katrina Hughes, Community Broadcasting Association of Australia, 'Australia's Right to Know Coalition of Media Companies calls on the Government to Amend Laws to Protect the Public's Right to Know' (Media Release, 26 June 2019) <https://www.cbaa.org.au/article/media-release-australias-right-know-coalition-media-companies-calls-government-amend-laws>.
[131] *Australian Security and Intelligence Organisation Act 1979* (Cth) s 34D.

138. The Law Council considers that there is a need for improved safeguards in relation to warrants authorising investigative action, noting in particular the prominent public interest considerations that exist in relation to warrants concerning journalists and media organisations. The importance of the 'up front' review process for a warrant request should not be understated and is an essential step in determining whether the proposed intrusion of privacy is lawful, necessary and appropriate. The Law Council submits that there is a need for greater oversight in this regard, especially independent scrutiny of the sufficiency and proprietary nature of the information provided to support search warrants relating to journalists and media organisations.

139. The Law Council therefore recommends a multifaceted approach to strengthening safeguards within the warrant process concerning journalists, and is supportive of moves to create an adversarial environment in which a greater degree of scrutiny is brought to bear on the grounds advanced for seeking a warrant and for claiming that it is a necessary and justified intrusion into the privacy of those likely to be affected. The Law Council considers that this could potentially be achieved with the introduction of a public interest requirement, which is to be considered by a judge with appropriate expertise and superiority to hear matters of public interest, and the introduction of a PIA or PIM scheme. These improved scrutiny measures are discussed individually below.

Public interest requirement

140. The Law Council submits that the Committee should give consideration to whether a public interest requirement should be applied when determining whether to issue a warrant in relation to journalists and media organisations, either as the suspect of an offence or as a third party in possession of information relevant to an investigation, similar to what occurs pursuant to the TIA Act. Under section 180T of the TIA Act, the issuing authority of a journalist information warrant must apply a public interest test that weighs up the public interest in issuing the warrant against the public interest in protecting the confidentiality of the identity of the source.

141. The Law Council suggests that a legislative requirement that a decision-maker must take into account public interest elements when determining whether to issue a warrant authorising investigative action of a journalist or media outlet would be a positive addition to the existing scheme. This requirement could be complemented by the introduction of an advocate to assist in the determination of public interest factors, as outlined below

The 'issuing officer'

142. As noted above, under the Crimes Act a magistrate, a justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest, may issue warrants, including those which relate to journalists and media organisations.[132]

143. The inclusion of a legislated public interest requirement for the issuance of search warrants relating to journalists and media organisations requires a balancing of competing interests between the disclosure and non-disclosure of certain information.

144. As this requirement would mandate the careful consideration of matters of significant public interest, the Crimes Act should require that the issuing officer of a search warrant pertaining to journalists and media organisations is a judge of a superior court of record rather than that which is currently required under section 3C of the Crimes Act.

[132] *Crimes Act 1914* (Cth) s 3C definition of 'issuing officer'.

145. The Law Council considers that in the exceptional case where a journalist or media organisation is the subject of a search warrant, these requirements which place greater scrutiny on the warrant issuance process would be unlikely to hinder the efficacy of an investigation and serve to strike the appropriate balance between the proper exercise of law enforcement powers and a strong and free press.

Public Interest Advocate or Public Interest Monitor

146. It is submitted that the introduction of a PIA or Public Interest Monitor PIM regime could serve to promote an adversarial process in a manner similar to what occurs under the TIA Act for journalists in terms of mandatory data retention. Such an approach could be valuable where it assists the decision maker to review the information contained in warrant application more thoroughly and from more than one perspective.

147. The Law Council notes however, that there is little value in introducing a PIA or PIM into the warrant application process if the result, in practice, is simply the transfer of responsibility for reviewing and interrogating the warrant application from the ultimate issuer of the warrant to the PIA or PIM. The decision maker must still scrutinise the information at hand. Similarly, it is important that the role of the PIA or PIM carries proper weight and does not become a 'rubber stamp' process.

148. Despite the benefits of the above approach, the Law Council has reservations about the way in which the current PIA regime operates under the TIA Act. These concerns are detailed further below. In light of these observations, the Law Council would only support the introduction of a PIA or PIM regime in relation to investigative warrants where increased transparency mechanisms are in place. This would include measures such as formal training for advocates, transparency regarding their appointments and annual public reporting on the number of contested cases and success rates.

Recommendation:

- **The determination of warrants authorising investigative action of journalists or media organisations, either as the suspect of an offence or as a third party in possession of information relevant to an investigation would be improved through the:**
  - **introduction of a legislative public interest test similar to which occurs under the test provided in section 180T of the *Telecommunications (Interception and Access) Act 1979* (Cth);**
  - **requirement that a 'issuing officer' is a judge of a superior court of record rather than that currently provided in section 3C of the Crimes Act; and**
  - **adoption of a Public Interest Advocate or Public Interest Monitor regime that includes appropriate transparency and accountability mechanisms.**

Accessing of electronic data on journalists' devices

149. Recent legislative changes introduced by the Assistance and Access Act and the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (**Data Retention Act**) have significantly increased the powers of law enforcement and intelligence agencies to access the data, and encrypted data, of Australians.

150. The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in 2013 that surveillance of journalists can serve to stymie freedom of the press and – by implication – limit the right to freedom of opinion and expression:

> *Journalists are … particularly vulnerable to becoming targets of communications surveillance because of their reliance on online communication. In order to receive and pursue information from confidential sources, including whistleblowers, journalists must be able to rely on the privacy, security and anonymity of their communications. An environment where surveillance is widespread, and unlimited by due process or judicial oversight, cannot sustain the presumption of protection of sources. Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.*[133]

Mandatory national data retention regime

151. The Data Retention Act introduced amendments to the TIA Act to establish a mandatory national data retention regime which commenced on 13 October 2015.

152. The retention of metadata in itself has been criticised as potentially having chilling effect on freedom of expression and association, especially as the regime in Australia does not require pre-access approval, with the exception of journalists.[134]

153. In the course of performing their function, journalists rely on receiving information from the public and in some cases whistleblowers. In the view of the Law Council, greater safeguards and accountability measures are required in the data retention scheme, particularly in relation to journalist warrants and PIA system, to ensure that the information stored on journalists' devices is adequately protected from covert and intrusive access by law enforcement agencies, particularly where the objective of such access is to identify the journalist's source.

154. Under the data retention scheme, a higher threshold is required for access to telecommunications data where metadata was being sought in relation to a journalist for the purpose of identifying that journalist's source. Division 4C of Chapter 4.1 of the TIA Act sets out the requirements and procedure for a law enforcement agency to apply for a journalist information warrant to be issued. The applications for this type of warrant are also subject to the scrutiny of the PIA.

155. The Law Council considers that access to telecommunications data, including journalists, must be governed by a robust legislative regime to ensure access is only permitted when the public interest in detecting and addressing serious criminal activity outweighs the public interest in ensuring Australians can conduct their lives free from

[133] Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 23rd sess, UN Doc A/HRC/23/40 (17 April 2013), 52.
[134] Digital Rights Watch, *State of Digital Rights Report 2018* (May 2018) 4.

unnecessary intrusion of their privacy by the State. It is important that the regime provides safeguards against the wilful, systematic degradation of human rights in the digital era such as the fundamental human right to privacy.

156. Just as there is a requirement for a warrant to be issued before access can be permitted to the telecommunications data of a journalist, the Law Council holds the view that the same requirement for a warrant should apply in relation to accessing the metadata of all members of the Australian community.[135] Furthermore, the Law Council considers that greater legislative safeguards are required to ensure that warrants are required in instances where the authorisation was issued for the purpose of identifying a journalist's source.

157. According to the Annual Report of the Department of Home Affairs during the reporting period of 2016-2017, there were no authorisations made for the issue of a journalist information warrant.[136] This is not to say that access was not obtained by a law enforcement agency to metadata pertaining to a journalist. In the 2019 submission of the AFP to the PJCIS on its review of the mandatory data retention regime, it reveals that 58 authorisations were made in the year 2017-2018, yet only 2 journalist information warrants were issued in the same period.[137]

158. On 28 April 2017, the AFP Commissioner, Andrew Colvin APM OAM, held a press conference to disclose that a breach of the TIA Act had occurred within the AFP. The breach occurred within the Professional Standards Unit (**PRS**) and involved access by officers from the AFP to the telecommunications data of a journalist used to identify the journalist's source without a warrant. This breach of the TIA Act was subsequently investigated by the Ombudsman who found there were four discreet authorisations associated with this breach.[138]

159. The report of the Ombudsman stated there were four main reasons for the breach of the TIA Act by the AFP in failing to apply for a journalist information warrant:

- there was insufficient awareness surrounding the journalist information warrant requirements within the PRS;
- within the PRS, a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers;
- the AFP relied heavily on manual checks and corporate knowledge as it did not have in place strong system controls for preventing applications that did not meet relevant thresholds; and
- the guidance documents were not effective as a control to prevent this breach.[139]

160. The Ombudsman subsequently recommended that the AFP immediately review its approach to metadata awareness raising and training to ensure that all staff involved in

[135] Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (18 July 2019) 19 [67].
[136] Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 (Cth) – Annual Report 2016-2017* (2017) 51.
[137] Australian Federal Police, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (2019) Table 7.
[138] Michael Manthorpe PSM, Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979* (October 2017) 3.
[139] Ibid 2.

exercising metadata powers have a thorough understanding of their responsibilities and obligations under Chapter 4 of the TIA Act.[140]

161. The Ombudsman also observed that 'there is ambiguity surrounding the circumstances of when a journalist information warrant is required' in that if an authorisation was issued for the purpose of identifying a journalist's source, but not made directly in relation to the journalist or their employer, a warrant is not required, even though the information may still reveal the source of the journalist to the AFP.[141]

162. This may serve to highlight a practical difficulty in that without first accessing and examining the telecommunications data, it may not be possible to identify if the data is that of the journalist, their employer or is capable of being used to identify a journalist's source. As with the data retention scheme generally, it is not possible for the journalist, or anybody else, to discover that their data is being accessed unlawfully.

163. The Law Council agrees with the observation made by the Ombudsman that the definition of a 'particular person' for the purpose of subsection 180H(1) of the TIA Act to be either a 'person working in a professional capacity as a journalist' or 'an employer of such a person' is too narrow. Rather the section should focus on the intention of identifying a journalist's source and should include a paragraph that captures 'or any other person whose telecommunications data may reasonably be believed to be used to identify any journalist's source'.

164. The Law Council also considers that the recent use of the new powers conferred by the Assistance and Access Act by the AFP to execute search warrants on the office of the ABC and the residence of a News Corporation journalist illustrates that the protection afforded by the journalist information warrant scheme can be easily bypassed. The utility of the provisions in the TIA Act devised to protect freedom of speech and protect journalistic sources has effectively been rendered ineffectual with reforms introduced by the Assistance and Access Act. A search warrant that is executed on a journalist now enables the police, pursuant to the amended section 3F of the Crimes Act to access computers and information that under the Data Retention Act which would require the issuance of a journalist information warrant.[142]

165. In these circumstances, the Law Council considers that the legal protection afforded to journalists and freedom of expression should be strengthened generally and the data retention regime is one area that could benefit from reform, especially given the implications of the Assistance and Access Act.

Recommendations:

- **Any access to retained telecommunications data should be authorised by a warrant issued by an independent court or tribunal.**
- **Section 180H of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to include a paragraph so that a journalist information warrant is required for the authorisation of access to the telecommunications data of any person that may reasonably be believed as being used to identify a journalist's source.**

[140] Ibid.
[141] Ibid 3.
[142] Josh Taylor, 'Australia's Anti-Encryption Laws Being Used to Bypass Journalist Protections, Expert Says', *The Guardian* (online, 8 July 2019) <www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says>.

Increased transparency and accountability: Public Interest Advocates

166. The Data Retention Act established PIAs, the powers, role and function of which are set out in the *Telecommunications (Interception and Access) Amendment (Public Interest Advocates and Other Matters) Regulation 2015*. The Law Council understands that currently there are five PIAs.[143]

167. Appointed by the Prime Minister, a PIA receives proposed journalist information warrant requests made by the Director-General of Security or enforcement agencies.[144] Upon receipt of such a request, the PIA may consider the proposed request or application and must, as soon as reasonably practicable, advise the applicant that he or she will or will not prepare a submission in relation to the proposed request or application. The PIA must also advise the applicant whether they will attend at the hearing of the application.[145]

168. After a decision has been made to issue, or refuse to issue, a journalist information warrant, or a request or application for such a warrant is withdrawn, PIA must return all documents relating to the proposed request.[146]

169. The role of PIAs, as described by the Department of Home Affairs, is to:

> *promote the rights of a journalist to seek and impart information by independently considering and evaluating warrant applications and providing independent submissions in the warrant application process.*[147]

170. Recent reports have raised concerns about the secretive, covert nature of the way in which the PIA system operates. It has been said that it 'allow[s] the authorities to fly under the radar'.[148] The Law Council notes that at no point is the PIA required to inform the journalist to which the warrant relates, or their media employer.[149]

171. Furthermore, section 182A of the TIA Act makes it an offence, punishable by two years' imprisonment, for a person to disclose or use information about:

- whether a journalist information warrant (other than such a warrant that relates only to section 178A) has been, or is being, requested or applied for;
- the making of such a warrant;
- the existence or nonexistence of such a warrant; or
- the revocation of such a warrant.

172. Permitted disclosure of information relating to journalist information warrants is permissible in only a limited number of circumstances, such as to enforce the criminal law or to an IGIS official in relation to the exercise of its statutory powers and duties.[150]

---

[143] Media Watch, 'Journalist Information Warrants' (ABC, 22 July 2019) <https://www.abc.net.au/mediawatch/episodes/jiw/11335902>.
[144] *Telecommunications (Interception and Access) Amendment (Public Interest Advocates and Other Matters) Regulation 2015* (Cth) cl 6, 7.
[145] Ibid cl 8(2), 10.
[146] Ibid cl 12.
[147] Media Watch, 'Journalist Information Warrants' (ABC, 22 July 2019) <https://www.abc.net.au/mediawatch/episodes/jiw/11335902>, citing Email from Department of Home Affairs (14 June 2019).
[148] Ibid, citing Email from Dr Joseph Fernandez, Curtin University (18 July 2019).
[149] Media, Entertainment and Arts Alliance, 'Journalist Information Warrants' (2 May 2019) <https://pressfreedom.org.au/journalist-information-warrants-d47b402ae071>.
[150] *Telecommunications (Interception and Access) Act 1979* (Cth) s 182B.

173. Noting the above concerns regarding the operation of the PIA scheme, the Law Council considers that there is a need for improved transparency and accountability in relation to the appointments and activities of PIAs.

Recommendations:

- **Annual reporting to the Parliament should occur, which includes the:**
  - **number and identity of Public Interest Advocates (PIA);**
  - **number of cases where a PIA contested a journalist warrant;**
  - **number of cases where a PIA attended the hearing of an application for a journalist warrant; and**
  - **number of journalist warrants that were successfully contested by a PIA.**
- **The Committee should obtain the advice of former and current PIAs as to whether they are able to effectively perform their roles as defined in the *Telecommunications (Interception and Access) Amendment (Public Interest Advocates and Other Matters) Regulation 2015* (Cth).**

Powers introduced and increased by the Assistance and Access Act 2018

174. The Law Council has previously expressed concern about measures introduced by the Assistance and Access Act, many of which remain unaddressed.[151] As stated above, the amendments introduced allowed the AFP when executing the search warrant at the ABC headquarters to 'add, copy, delete or alter' the material on the ABC's computers.[152] The AFP was authorised to change, tamper and destroy other ABC computer files as long as it was necessary to access the data they were seeking.[153]

175. Moreover, in the context of the current inquiry, the Law Council is concerned that the threshold for telecommunications interception through a computer access warrant has been lowered. The granting of wider circumstances in which investigators may gain access to journalists' devices, and the information and the personal data contained therein, can translate to an encroachment on the freedom of the press, as journalists' ability to protect their sources may be undermined.

176. In the Law Council's submission on the Assistance and Access Bill, it raised its concern that attaching telecommunications interception power to computer access

[151] See Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (18 October 2018); Law Council of Australia, Submission No 4 to Parliamentary Joint Commission on Intelligence and Security, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (23 January 2019); Law Council of Australia, Submission No 4.1 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (20 February 2019).
[152] Riana Pfefferkorn, Standard Centre for Internet and Society, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Amendments Made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (14 June 2019) 2.
[153] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) sch 3, inserting section 3F(2A)(B) to the *Crimes Act 1914* (Cth).

warrants involves a reduction in the threshold for telecommunications interception generally.[154]

177. Before the reforms, to issue a telecommunications service warrant under sections 9 or 9A of the TIA Act, the Attorney-General must have been satisfied that a telecommunications service was being or was likely to be used by a person engaged in or likely to engage in *activities prejudicial to security*. Whereas, to issue a computer access warrant under 25A of the ASIO Act, the Attorney-General must be satisfied that the data will assist the collection of intelligence in respect of a matter that is *important in relation to security.*

178. By the Assistance and Access Act inserting paragraphs 25A(4)(ba) (computer access warrants), 27A(3B)(g)-(h) (foreign intelligence warrants) and 27E(2)(d) (identified person warrants) into the ASIO Act, which allow for interception of communication passing over a telecommunications system, the threshold appears to be lowered from 'prejudicial to security' to 'a matter is important in relation to security'.

179. The Law Council does not consider that the potential lowering of the threshold has been demonstrated to be necessary and proportionate. The Law Council therefore recommends that a computer access warrant which allows the interception of a communication passing over a telecommunications system only be authorised by the Attorney-General if the Attorney-General is satisfied that the telecommunications service is being or is likely to be used for purposes prejudicial to security.

180. In addition, under the TIA Act where a law enforcement agency applied to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service, the Judge or nominated AAT member must be satisfied that, for example, information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which (i) the particular person is involved; or (ii) another person is involved with whom the particular person is likely to communicate using the service.[155] Serious offences generally include offences punishable by imprisonment for life or for a period or a maximum period of at least seven years under section 5D of the TIA Act.

181. The Assistance and Access Act introduced section 27A, the effect of which was the lowering of this threshold so that telecommunications interception may be permitted as part of a computer access warrant for a 'relevant' offence, defined in subsection 6(1) of the *Surveillance Devices Act 2004* (Cth) (**SDA**) as a Commonwealth offence, or a state offence with a federal aspect, that is punishable by imprisonment for a minimum of three years, or an offence otherwise prescribed in section 6(1) or by the regulation. This is a significant increase in the powers of law enforcement agencies, which does not appear to have been justified as a necessary and proportionate response.

182. While the Law Council recognises the different features of telecommunication intercept warrants and computer access warrants, in the absence of evidence to suggest why amendments to existing thresholds in relation to telecommunications interception should be lowered, the TIA Act should be amended so that the former thresholds apply for the purposes of the new computer access warrants in the ASIO Act and SDA.

---

[154] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (18 October 2018) 40-1 [119]-[121].
[155] *Telecommunications (Interception and Access) Act 1979* (Cth) s 46(1)(d).

Recommendations:

- **The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended so that:**
  - **a computer access warrant, foreign intelligence warrant or identified persons warrant allow the interception of a communication passing over a telecommunications system only when authorised by the Attorney-General if the Attorney-General is satisfied that the telecommunications service is being or is likely to be used for purposes prejudicial to security; and**
  - **telecommunications interception under a computer access warrant should be limited to relevant offences under the *Surveillance Devices Act 2004* (Cth) that are serious offences under the *Telecommunications (Interception and Access) Act 1979* (Cth).**