Law Council
OF AUSTRALIA

Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)

Parliamentary Joint Committee on Intelligence and Security

16 July 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
- President-elect, (vacant)
- 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 acknowledges the assistance of its National Criminal Law Committee in the preparation of this submission, as well as input from the Business Law Section's Privacy Law Committee.

Introduction

1. The Law Council is grateful for the opportunity to contribute to the Parliamentary Joint Committee on Intelligence and Security's (**Committee**) review of the amendments introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**Assistance and Access Act**).

2. The Law Council recognises that there is significant value to public safety in allowing law enforcement and national security agencies faster access to encrypted information where there are threats to national security or in order to prevent the commission of serious criminal offences. The Law Council also acknowledges that there is merit in facilitating prompt international cooperation and assistance to deal with serious crimes which occur across multiple jurisdictions.

3. The principal objective of the amendments introduced by the Assistance and Access Act was centred on the legitimate aim of increasing public safety by providing faster access to encrypted data. However, the primary concern of the Law Council is that the measures introduced by the legislation must always be reasonable, necessary and proportionate to that aim by including appropriate safeguards, controls, clarity and certainty in the legislation.

4. The Law Council notes that the Committee has previously conducted an inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (**Assistance and Access Bill**) and the Advisory Report of the Committee was tabled in Parliament on 5 December 2018.[1] In response to the recommendations contained in that report, a number of amendments were introduced by the Government to the Assistance and Access Bill which were then passed by Parliament on 6 December 2018. One of the amendments made to the Assistance and Access Bill required the referral of the Assistance and Access Act to the Committee for review and inquiry, with the Advisory Report of the Committee due in April 2019.

5. The April 2019 Advisory Report of the Committee stated that the focus of that particular inquiry was on 'clarifying the intent of the recommendations made in its 2018 Report and to advise the Parliament on the extent to which those recommendations were addressed'.[2] The Committee acknowledged the many submissions received and the evidence given during both the 2018 inquiry into the Assistance and Access Bill and the 2019 inquiry into the Assistance and Access Act. The Committee went on to state that, given the timing of the then approaching federal election and of this current statutory review now being undertaken by the Committee, the Committee did not to seek to respond to the matters raised in the submissions and evidence given by stakeholders in its Advisory Report dated 4 April 2019.[3]

6. However, the Law Council welcomes the three recommendations that were made by the Committee in that report, namely that:

   (a) section 187N of the Assistance and Access Act be amended to require the Committee's review of the amendments made by the Assistance and Access Act by June 2020;

[1] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018).
[2] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Advisory Report, April 2019).
[3] Ibid 4 [1.17].

(b) sufficient resources be made available to the Independent National Security Legislation Monitor (**INSLM**) to enable the review of the amendments made by the Assistance and Access Act; and

(c) the Government continues to ensure that the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman (**Ombudsman**) have sufficient resources to ensure that they can properly execute their additional responsibilities under the Assistance and Access Act.

7. The Law Council also acknowledges that the Government amendments did make some of the necessary improvements to the Assistance and Access Bill. In particular, there has been some improvement to record-keeping, inspection and reporting requirements, and have introduced important accountability and oversight measures.

8. However, the Law Council considers that there are a number of outstanding concerns (which the Government amendments have not addressed or have been addressed insufficiently) that are set out in the submission and supplementary submission of the Law Council previously lodged with the Committee dated 23 January 2019[4] and 20 February 2019.[5] These earlier submissions are included as **Attachment A** and **Attachment B** respectively, for the benefit of the Committee.

9. The Law Council maintains the previous recommendations made in earlier submissions which provide comment on the amendments sought to be introduced by the Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 (Cth) (**the Miscellaneous Amendments Bill**).

Reporting by the Commonwealth Ombudsman

10. In addition, the Law Council notes that the inspecting and reporting role held by the Ombudsman appears to be impeded by the ability for the Minister for Home Affairs to delete information in an Ombudsman's report where that information could reasonably be expected to:

(a) prejudice an investigation or prosecution; or

(b) compromise any interception agency's operational activities or methodologies.[6]

11. The Law Council supports the views of the Ombudsman that this power of redaction is unnecessary and is inconsistent with the Ombudsman's role as an independent and impartial office. The Law Council endorses the recommendation of the Ombudsman in this regard and supports its recommendation to the Committee to remove the redaction power contained at subsection 317ZRB(7) of the *Telecommunications Act 1997* (Cth).[7]

[4] 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).
[5] 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).
[6] *Telecommunications Act 1997* (Cth) s 317ZRB(7).
[7] Commonwealth Ombudsman, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (July 2019) 4.

Interaction with foreign laws

12. As per the Terms of Reference of the current inquiry by the Committee, the remainder of this submission will focus on the interaction of the amendments introduced by the Assistance and Access Act with foreign laws – in particular the United States *Clarifying Lawful Overseas Use of Data Act*[8] (**CLOUD Act**) and the European Union's (**EU**) *General Data Protection Regulation* (**GDPR**).[9]

Interaction with the United States CLOUD Act

13. The CLOUD Act was enacted on 23 March 2018 by the passing of the *Consolidated Appropriations Act of 2018* by the 115th United States Congress.[10]

14. The CLOUD Act amends the United States Code (**US Code**) to improve law enforcement access to data stored across borders by, in effect, removing the previous prohibition on providers of electronic communication services from disclosing the contents of electronic communications to foreign governments[11] in certain conditions.[12]

15. The CLOUD Act creates provisions for the provider of an electronic communication service or remote computing service operating in the United States (**US**) to disclose to a 'qualifying foreign government' that is party to an 'executive agreement' with the US the contents of electronic communication of a national or resident of the foreign government directly to a foreign investigative body, such as the Australian Federal Police (**AFP**) in certain circumstances.[13]

16. This would enable, for instance, Facebook (operating from within the US) to provide the contents of electronic communications of an Australian resident that would assist in the investigation of a terrorism-related (or other serious criminal) offence, to the AFP without the AFP having to seek that information through the current process required by the mutual legal assistance treaty (**MLAT**).[14]

17. The CLOUD Act achieves this by amending the *Electronic Communications Privacy Act*[15] (**ECPA**) which regulates the US service provider's disclosure of information about their users, and previously precluded US providers from disclosing user's metadata or communications content to foreign governments.

18. For an Australian law enforcement agency to access the provisions of the CLOUD Act, there needs to be an 'executive agreement' in place between Australia and the US governing access by Australian law enforcement agencies to the data. A requirement of any 'executive agreement' is that the US Attorney General, with the concurrence of the Secretary of State, must determine that the domestic law of Australia 'affords robust substantive and procedural protections for privacy and civil

---

[8] *Clarifying Lawful Overseas Use of Data Act,* HR 4943, 115th Congress (2017-2018).
[9] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*').
[10] *Consolidated Appropriations Act of 2018*, Pub L No 115-141, § 102, 132 Stat 1213.
[11] See *Microsoft Corp. v United States,* 829 F 3d 197, 210 (2d Cir, 2016).
[12] 18 USC § 2713.
[13] Ibid §§ 2702, 2703.
[14] The executive agreements made in accordance with the CLOUD Act only authorise the foreign government to access data of foreigners located outside of the United States.
[15] *Electronic Communications Privacy Act of 1986*, HR 4952, 99th Congress (1985-1986).

liberties in light of the data collection and activities of the foreign government that will be subject to the agreement' as assessed by a number of factors listed.[16]

19. The Law Council notes and agrees with the submission of the Digital Industry Group Inc (which includes representatives from Amazon, Facebook, Google, Oath, and Twitter) on the Assistance and Access Bill, which noted:

> *If our data access regime doesn't contain sufficient safeguards for user privacy, there is a chance that the US Congress, for example, will not approve a treaty with Australia under the CLOUD Act which will interfere with legitimate law enforcement investigations.*[17]

20. Furthermore, the Law Council notes that an executive agreement cannot 'create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data'.[18]

21. Each individual request must be particularised (targeting a specific person, account, address, personal device or other identifier, based on 'articulable and credible facts') and be subject to 'review or oversight by a court, judge, magistrate or other independent authority'.[19]

22. The Law Council considers that the current law in Australia as it relates to storing and accessing telecommunications data will be insufficient to allow Australia to qualify for entry into an 'executive agreement' with the US. This means that law enforcement agencies in Australia will be restricted to seeking access to data held by a service provider in the US through the existing and time consuming MLAT process.

23. The reason for this is that irrespective of what laws Australia may pass, they are insufficient on their own to compel a service provider in the US to do anything not authorised by US law. The sovereignty of both countries is well established and reinforced in this context by each country ratifying the *Budapest Convention on Cybercrime*.[20]

24. Further, the amendments introduced by the Assistance and Access Act do not meet some of the specific criteria required by the CLOUD Act that permit the US to enter an 'executive agreement' with Australia because the legislation arguably fails to meet the following requirements of the CLOUD Act:

    a) the order issued by the foreign government should be specific and identify the relevant individual, account, address or personal device or another specific identifier;
    b) the agreement cannot create an obligation that cannot be fulfilled under US law. In this context, the requirements under the Assistance and Access Act and the CLOUD Act clearly differ, as the US law does not allow for the mandating of the decryption of data as is now permitted under Australian law; and
    c) the CLOUD Act requires that the order issued by the foreign government 'be subject to review or oversight by a court, judge, magistrate or other independent authority prior to, or in proceedings regarding, enforcement of the order' and this

[16] 18 USC § 2523(b)(1).
[17] Digital Industry Group Inc., Submission No 78 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (19 October 2018) 3.
[18] 18 USC § 2523(b)(3).
[19] 18 USC § 2523(b).
[20] *Convention on Cybercrime*, opened for signature 23 November 2011, ETS No 185 (entered into force 1 July 2004).

condition may not be adequately addressed by the amendments introduced by the Assistance and Access Act.

25. It could be argued that section 317ZH places a restriction on a technical assistance notice (**TAN**) or a technical capability notice (**TCN**) from being used to access data or communications that would not be permitted by the issue of a warrant. This may arguably ensure sections 317L and 317T do, in effect, require a TAN or TCN to relate to a specific identifiable 'person, account, address, or personal device'.

26. However, the second, more problematic issue is the inconsistency of the obligations in relation to encryption imposed by the Assistance and Access Act and the US federal law, contained in the *Communications Assistance for Law Enforcement Act 1994* (US) (**CALEA**).[21] This Act does not preclude a carrier from deploying an encryption service for which it does not retain the capacity to decrypt if and when requested by law enforcement to do so. That is, it does not 'mandate that US providers of encrypted communications, devices, and storage services be able to decrypt communications for law enforcement access'.[22] In these circumstances, as argued by Riana Pfefferkorn, Associate Director of Surveillance and Cybersecurity at the Stanford Centre for Internet and Society in the United States, citing §2523(b)(3) of the US Code: 'Any executive agreement with Australia is flatly barred from "creating any obligation that providers be capable of decrypting data"'.[23]

27. Irrespective of the amendments introduced by the Assistance and Access Act in Australia, the provisions of the CLOUD Act will not allow US service providers to provide technical assistance beyond their existing obligations under CALEA. Therefore, even under the existing MLAT scheme a US service provider could not be compelled to comply with a TCN or a TAN issued under the Assistance and Access Act.

28. A further hurdle to Australia being able to form an 'executive agreement' with the US under the CLOUD Act is that the Assistance and Access Act does not provide sufficient requirements for the independent judicial oversight of the issuance of a TAN or a TCN.

29. The Law Council maintains that with the exception of the procedure to issue a TCN, the other measures introduced by the Act are not subject to any form of consideration by an independent judicial officer, notwithstanding the 'general limits' provided by section 317ZH of the Assistance and Access Act. In the case of TCNs, there is a requirement for the exercise of discretion by the Attorney-General who, while Australia's first Law Officer, is not a demonstrably independent party, and is still a member of the Executive.

30. While there is some limited capacity for the courts to make orders in relation to the disclosure, protection, storage, handling and destruction of information obtained pursuant to a TAN, TCN or a technical assistance request (**TAR**),[24] there is no provision for the judicial review of the actual decision to issue the TAN, TCN or TAR.

[21] *Communications Assistance for Law Enforcement Act of 1994*, Pub L No 103-414, 108 Stat 4279, codified at 47 USC § 1001-10.
[22] Riana Pfefferkorn, Stanford Centre for Internet and Society, Submission No 35.2 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (13 November 2018) 7.
[23] Ibid.
[24] *Telecommunications Act 1997* (Cth) s 317ZFA.

Interaction with the laws of the European Union

31. The EU's GDPR commenced on 25 May 2018. The GDPR sets a number of restrictions on the processing and transfer of 'personal data'[25] out of the EU, including in response to court orders issued by countries outside of the EU. The GDPR can apply to organisations operating in Australia, where the organisation in question:

    (a) is processing personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not[26]; or

    (b) is offering of goods or services to data subjects in the EU or monitoring of their behaviour as far as their behaviour takes place within the EU.[27]

32. Where the GDPR applies to Australian entities and those entities carrying on business in Australia, it will do so as a matter of law and those in breach of obligations may be subject to law enforcement. Companies subject to the GDPR must ensure that the software, hardware and data centres they use include appropriate safeguards to protect personal data.

33. Notwithstanding that a TCN or a TAN is unable to force a service provider to comply with a notice if it could potentially lead to a 'systemic vulnerability' or 'systemic weakness' to do so, there remains concern about the potential for this to nonetheless occur where a provider attempts to comply, and compliance with the notice potentially compromises the security of personal information.

34. This is contrary to the provisions of the GDPR which requires service providers and other controllers of data to implement appropriate technical and organisational measures so as to implement the data protection principles and provide protection and security for the 'personal data' within the EU. The aims of the GDPR and the requirements of a TCN or TAN to remove or limit the security measures required to protect privacy may be difficult to reconcile.

35. While there is a defence under the Assistance and Access Act to complying with a TAN or a TCN for a 'designated communications provider other than a carrier or carriage service provider' where it would cause contravention of a foreign law,[28] this exemption appears to only apply to acts done outside of Australia. This means that acts done within Australia are not covered by the exemption and therefore compliance with a TCN and TAN may bring the service provider into conflict with a foreign law such as Article 32 of the GDPR.[29]

36. The Law Council has additional concern about the difficulty of defining 'do an act or thing in a foreign country' given the transnational operation of the technology that a TCN or TAN may target. It is conceivable that a TCN or TAN may require a designated communications provider operating in Australia to provide assistance which, although it only requires an employee to do an act or thing in Australia, the software is partially

[25] 'Personal data' is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person: *GDPR* art 4(1).
[26] Ibid art 3(1).
[27] Ibid art 3(2).
[28] *Telecommunications Act 1997* (Cth) s 317ZB(5).
[29] Article 32(1) of the *GDPR* deals with 'Security of processing' and requires a controller and the processor of personal data to 'implement appropriate technical and organisational measures to ensure a level of security appropriate', including, *inter alia*, 'the pseudonymisation and encryption of personal data': *GDPR* art 32(1).

located in the foreign country and/or executed or modified remotely from Australia. This leaves open an ambiguity as to whether the 'doing of the act' (being the execution or modification of the software) is occurring in Australia or the foreign country, leading to ambiguity as to whether the defence applies.

37. Article 48 of the GDPR allows any judgment of a court or tribunal, 'and any decision of an administrative authority' of a country to be recognised within the EU, but only where there is an 'international agreement' in force between Australia and the EU or the applicable Member State of the EU.

38. Personal data may possibly be released from the EU pursuant to an order issued under the Assistance and Access Act under Article 49 of the GDPR, which provides that in the absence of an authorisation being made in accordance with either Article 45 or 46, there is still discretion where 'the transfer is necessary for important reasons of public interest'.[30] It may be that an argument could be made that a serious threat to Australian security would be 'important reasons of public interest'.[31]

39. The difference in approach to the protection of personal data in the EU and Australia is perhaps emblematic of the broader differences being adopted between Australia and the EU in relation to balancing the fundamental human right to privacy and the need for laws that address the need to provide for effective national security measures. In the EU, there is greater protection being given to the fundamental human right of privacy, as reflected in the enactment of the GDPR. However, in Australia, the laws relating to encryption are increasing the capacity of law enforcement to overcome one of the means by which privacy in electronic communications can be protected.

[30] *GDPR* art 49(1)(d).
[31] Such a reasons may also comply with the *GDPR*. This direction deals with the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences and restricts such access to being in accordance with the laws of the EU, and therefore the GDPR.

Law Council
OF AUSTRALIA

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)

Parliamentary Joint Committee on Intelligence and Security

23 January 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 1 January 2019 are:

- Mr Arthur Moses SC, President
- Mr Konrad de Kerloy, President-elect
- Ms Pauline Wright, Treasurer
- Mr Tass Liveris, Executive Member
- Dr Jacoba Brasch, Executive Member
- Mr Tony Rossi, Executive Member

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

Acknowledgement

In the preparation of this submission, the Law Council is grateful for the assistance of:

- its National Criminal Law Committee; and
- its Privacy Law Committee of the Business Law Section.

Executive Summary

1. The Law Council welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (**the Committee**) inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**the Act**) with specific reference to Government amendments introduced and passed on 6 December 2018 (**the Government Amendments**).

2. The Law Council acknowledges that the Government amendments have made some the improvements to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (**the Bill**). Notably, they have improved record-keeping, inspection and reporting requirements, and have introduced important accountability and oversight measures.

3. However, the Law Council considers that there are a number of areas which the Government amendments have not addressed, or which have been addressed in an insufficient manner. The key outstanding issues, in the view of the Law Council, are detailed below.

4. First, the Government amendments have not addressed, to any extent, the uncertainty regarding the potential for law enforcement or the Australian Security Intelligence Organisation (**ASIO**) to effectively detain individuals under the new powers in the Act, which can compulsorily require assistance to be provided to law enforcement or ASIO in certain circumstances. If a person is required to attend a place to provide information or assistance, this may arguably amount to detention of the person, particularly as they may be arrested on suspicion of the offence if they attempt to leave. This possibility of detention needs to be reconsidered with a view to ensuring that there are appropriate safeguards in place for detention, such as: allowing a person to contact a lawyer or family member; prescribing for maximum periods for giving assistance; requiring explanations of legal rights and responsibilities; the availability of interpreters where required and ensuring that the person is treated humanely and with respect for their human dignity.

5. Secondly, the Law Council considers that the voluntary assistance request and the technical assistance request (**TAR**) schemes, in addition to the technical assistance notices (**TAN**) and technical capability notices (**TCN**), should not be used as means of avoiding the important safeguard of a warrant. Where law enforcement agencies or ASIO would otherwise require authorisation or approval from the court, the Administrative Appeals Tribunal, or the Minister, they should not be able to make a voluntary assistance request or a technical assistance request and this should be made clear on the face of the legislation. The Law Council welcomes the Government amendment which broadens the application of the general limits, which previously only applied to TANs and TCNs, to TARs. It also welcomes the amendments to section 317ZH, as well as to the 'listed acts or things' for the purposes of industry assistance provisions, which seek to add clarity to the prohibition against the side-stepping of warrants. However, the Government amendments do not address the uncertainty regarding the potential for ASIO to make a voluntary assistance request requiring a provider to undertake certain acts or things, including telecommunications interception, for which they would otherwise require a warrant.

6. Thirdly, the Government amendments have not addressed the significant expansions of power for law enforcement and ASIO in relation to the proposed new computer access warrants, including:

(a) the ability to access telecommunications interception on the basis of lower thresholds than that which formerly applied;

(b) the ability to use force against persons or things to engage in telecommunications interception; and

(c) permitting telecommunications interception and temporary removal of computers and things for the purpose of entering premises rather than gaining access to relevant data.

7. The Law Council notes that the Government amendments appear to place time-limits on the removal of computers from premises and safeguards on the concealment of access provisions, however, the Law Council considers these amendments to be insufficient.

8. Fourthly, the decision-making powers in relation to Schedule 1 of the Act for industry assistance do not task the relevant decision maker, when making a 'reasonable and proportionate' determination, to determine whether perceived law enforcement or national security should outweigh the affected individuals' and businesses' reasonable expectations of confidentiality and privacy of communications. The Law Council considers that the decision-making criteria should be improved by including, for example: an express requirement that the decision maker must consider reasonable commercial interests of the provider to whom the notice relates, as well as a requirement to consider the fundamental right to privacy of affected individuals. Nonetheless, the Law Council welcomes the Government amendment requiring all Schedule 1 industry assistance notices, not just TANs and TCNs, to apply the same decision-making criteria. It also welcomes the addition of the express requirement of necessity to the decision-making criteria.

9. Lastly, the Act continues to allow for the conferral of civil and criminal immunities for providers that provide assistance to law enforcement or security agencies. In some cases, they would appear to allow a senior bureaucrat of ASIO to, for example, confer civil immunity. The Law Council considers that this measure has not been adequately justified and recommends that the conferral of civil immunity powers in the case of ASIO should be by the Attorney-General.

10. In addition to these outstanding issues which remain unaddressed by the Government amendments, the Law Council has detailed in this submission what it considers to be the key issues raised by the Government amendments, including but not limited to:

(a) the definition of 'serious Australian offences' and 'serious foreign offences';

(b) the definition of 'systemic weakness' and 'systemic vulnerability';

(c) the non-binding nature of the report and assessment by an expert and former judge on the decision of the Attorney-General to issue a TCN;

(d) the absence of judicial approval for Schedule 1 notices; and

(e) computer access warrants permitting telecommunications interceptions under emergency authorisations.

Improvements made on the Bill

Industry Assistance Notices

- The Government amendments require the Committee and Independent National Security Legislation Monitor (**INSLM**) to review of the operation of the amendments made by the Act.

- The Government amendments replaced the words '(but are not limited to)' with 'must be' in subsections 317L(3) and 317T(7), rendering the 'listed acts or things' under section 317E for TANs and TCNs exhaustive.

- State and Territory independent commissions against corruption were removed from the list of agencies who are deemed by the Act to be an 'interception agency' for the purposes of Part 15 of the *Telecommunications Act* 1997 (Cth) (**Telecommunications Act**), as was recommended by the Committee.[1]

- Subsection 317L(2A) has been introduced by the Government amendments to make it clear that TANs must not used to require designated communications providers (**DCP**) to build new capabilities.

- Subsection 317ZF(5A) permits an Ombudsman official to disclose information relating to a TAN, TCN or TAR which is in connection with the Ombudsman official exercising powers, performing functions or duties.

- Subsections 317ZF(5B)–(5C) allow for the authorised disclosure of TAR, TAN or TCN information to a State or Territory inspecting body.

- The Government amendments broadened the scope of subsection 317ZG(1) so that the general limits on Schedule 1 notices apply to TARs.

- A maximum 12-month time-limit for the operation of all TANs and TCNs has been introduced under new subsections 317MA(1A) and 317TA(1A).

- The Government amendments introduced section 317PA, requiring the Director-General of Security or the chief officer of an interception agency to consult with the DCP prior to the issuing of a TAN.

- Subsection 317W(1) requires the Attorney-General to give a DCP a written notice which sets out the proposal to give a TCN and invites the DCP to make a submission to the Attorney-General on the proposed TCN. The Attorney-General must consider the DCP's submission it if was provided within 28 days. This requirement also applies when the Attorney-General seeks to vary a TCN under section 317XA.

- Subsection 317WA(1) allows for a DCP, who has been given a consultation notice in relation to a proposed TCN, to give the Attorney-General a written request for an assessment of whether the TCN should be given.

- Subsection 317JAA(1) requires that the issuance of a TAR must be reasonable and proportionate, and compliance with the request is practicable and technically

[1] 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, ix [2.4].

feasible. The decision-making requirements now apply to all Schedule 1 industry assistance measures.

- The Government amendments introduced subsections 317JA(9)–(14), 317Q(10) and 317X(4) so that the decision-making criteria applies to the variation of TARs, TANs and TCNs.

- Subsections 317JB(1A)–(3A) and sections 317R and 317Z make clear that if a TAR, TAN or TCN is not reasonable or proportionate, or the compliance with the request is not practicable or technically feasible, the notice must be revoked.

- Subsections 317JC(g), 317RA(eb) and 317ZAA(eb) add the consideration of 'necessity' to the list of matters which must be considered when deciding whether the requirements imposed by a TAR, TAN or TCN are reasonable and proportionate.

- The notification requirements relating to TARs, TANs and TCNs have been improved by the requirement that ASIO or the Ombudsman (dependant on the interception agency which issued the notice) is notified within seven days about the issuance,[2] variation[3] or revocation[4] of a TAR, TAN or TCN.

- Subsection 317MAA(3) requires that when giving a TAN to a DCP, the Director-General of Security is under an obligation to inform the DCP of its right to make a complaint about the notice to the Inspector-General of Intelligence and Security (**IGIS**) (if TAN issued by Director-General of Security). Subsection 317MAA(4) places an obligation on the chief officer of an interception agency when giving a TAN to a DCP to inform the DCP of its right to make a complaint to the Ombudsman or an authority that is the State or Territory inspecting agency in relation to the interception agency.

- Subsections 317HAA(5)–(6), 317MAA(5)–(6), 317TAA(1)–(3) require that there must be a written record of oral advice from the relevant interception agency given to a DCP regarding their obligations relating a TAR, TAN or TCN.[5]

- Subsection 94(2BA) of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) requires that the annual report, prepared by the Director-General of Security for the Minister,[6] include a statement of the total number of TARs, TANs and TCNs issued during that period.[7] Subsection 94(2BB) requires that the Director-General of Security include TCNs in the annual report prepared for the Minister where the TCN was directed towards assisting ASIO, despite the fact that the Attorney-General, not the Director-General of Security, has authority to give TCNs. This means that the number of TARs, TANs and TCNs issued must be reported to Parliament as a whole.

- Paragraph 317ZS(1)(d) requires the Home Affairs Minister to include in its annual report under section 317ZS information on the kinds of serious Australian offences for which Schedule 1 powers are used in relation to. This means that this information is laid before Parliament.

---

[2] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* ss 317HAB, 317MAB, 317TAB ('*Assistance and Access Act*').
[3] Ibid ss 317JA(15)–(19), 317Q(12)–(14), 317X(6)–(8).
[4] Ibid ss 317JB(6)–(10), 317R(5)–(7), 317Z(3)–(5).
[5] Ibid ss 317HAA(5)–(6), 317MAA(5)–(6), 317TAA(1)–(3).
[6] *Public Governance, Performance and Accountability Act 2013* (Cth) s 46.
[7] *Australian Security Intelligence Organisation Act 1979* (Cth) s 94(2BA)(a)–(c).

- Section 317TAAA adds the requirement that the Attorney-General must obtain ministerial approval before the issuance of a TCN.

- The Government amendments appear to add clarity to section 317ZH regarding the prohibition against the side-stepping of warrants by adding the phrases 'that relates to an agency' and 'the agency, or an officer of the agency, would be required to have or obtain' to subsection 317ZH(1).

- The addition of paragraph 317E(1)(da) underscores that a TAR, TAN or TCN can only be issued to require one of the 'listed acts or things' be done by a provider where a valid warrant is in force to authorise the activity.

- New paragraph 570(3)(aa) and new subsections 570(4D) and 570(4C) in the Telecommunications Act provide for maximum penalties for body corporates and persons other than body corporates for contraventions of the civil penalty provisions in subsections 317ZA(1) and (2) for failing to comply with a requirement under a TAN or a TCN.

Computer Access Warrants

- Subsection 55(2B) of the *Surveillance Devices Act 2004* (Cth) (**SDA**) allows the Ombudsman to inspect records relating to the performance of Part 15 powers (e.g. issuance of a TAR, TAN, TCN) that have been used in connection with a surveillance device warrant, including computer access warrants. This amendment has the effect of including the new Part 15 powers within the Ombudsman's existing inspection regime. The Law Council supports this amendment as it appears to enhance oversight of the Schedule 1 industry assistance scheme.

- The Government amendments introduced subsection 64(2) in the SDA to provide for the circumstances in which the Commonwealth is liable to pay a person who has suffered loss or injury flowing from a computer access warrant.

- The Government amendments improve the authorised disclosures relating to general computer access intercept information under subsections 63AB(3)–(6) and 63AC(3)–(6) of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), as the measures permit authorised disclosures to the of the Ombudsman and IGIS.

Voluntary assistance to ASIO

- Subsections 21A(2) and (2A) of the ASIO Act require that an oral request for voluntary assistance under paragraph 21A(1)(a) must be in writing unless the making of the request should be made as a matter of urgency, would be prejudicial to security, or would be prejudicial to the operational security of the organisation, thus confining the circumstances in which a request may be made orally.

- Subsection 21A(3A) of the ASIO Act places an additional obligation on the Director-General to notify the IGIS that a request has been made, within seven days after the request was made.

- Subsection 94(2BC) of the ASIO Act requires that the total number of requests made under paragraph 21A(1)(a), as well as the total number of orders made under subsection 34AAA(2), is included in annual report prepared by the Director-General of Security for the Minister, which is tabled in Parliament.

Compulsory assistance to ASIO

- Subsections 34AAA(3A) and (3B) of the ASIO Act require the Director-General to make a written record of a verbal request within 48 hours.

- Subsection 34AAA(3C) of the ASIO Act requires that a request for compulsory assistance must be accompanied by a statement setting out the particulars and outcomes of all previous requests (if any) for the making of an order relating to the person specified in the current request.

- Subsection 34AAA(3D) and (3E) of the ASIO Act require that, if the grounds on which an order under section 34AAA was made have ceased to exist, the Director-General must inform the Attorney-General and, if the Attorney-General is also satisfied that the grounds have ceased to exist, the Attorney-General must revoke the order.

- Subsection 34(1A) of the ASIO Act provides that if an order was made under subsection 34AAA(2) in relation to the warrant (regarding a person with knowledge of a computer or a computer system to assist access to data), then the report must also include details of the extent to which compliance with the order has assisted the ASIO in carrying out its function. Subsection 34ZH(2) requires that if an order was made under subsection 34AAA(2) in relation to accessing data that was held in, or accessible from, a computer or storage device that was seized under section 34ZB, the report must also include details of the extent to which compliance with the order has assisted the ASIO in carrying out its functions.

Parliamentary Privilege

- Section 317RZ of the Act, section 27J of the SDA, section 3SA of the *Crimes Act 1914* (Cth) (**Crimes Act**) and section 202B of the *Customs Act 1901* (Cth) (**Customs Act**) are broad provisions which maintain that parliamentary privilege is not abrogated, rather than limited approach that only permits limited disclosures.

Recommendations regarding the Government Amendments

Industry Assistance Notices

- The definition of 'serious offences' should be consistent with the TIA in so far that 'serious offences' is defined as laws of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of seven years or more, rather than three years.

- Subsection 317G(6) be amended to replace the words '(but are not limited to)' with 'must be', as was done for subsections 317L(3) and 317T(7).

- Disclosure of TAR, TAN or TCN information to the Office of the Australian Information Commissioner (**OAIC**) and to the Australian Commission for Law Enforcement Integrity (**ACLEI**) be 'authorised disclosures' under subsection 317ZF(3) as is provided for in paragraphs 122.5(3)(iia) and (iii) of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth).

- The Act be amended to provide for a defence to the unauthorised disclosure of information in accordance with the Public Interest Disclosure Act 2013 (Cth) (**PID Act**) or the *Freedom of Information Act 1982* (Cth) (**FOI Act**).

- Section 317ZF be amended so that a request for disclosure from a DCP 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.

- The secrecy offence in subsection 317ZF(1) include an express harm requirement.

- Subsection 317ZG(1) be amended to prohibit a TAR, TAN or TCN from requesting or requiring any act or omission that might require a DCP to either implement or build any weakness or vulnerability into a current or proposed product or service.

- In the alternative, if the current definitions of 'systemic weakness' and 'systemic vulnerability' remain in the Act, the Law Council submits that terms 'whole class of technology' and 'connected' be defined in the Act.

- 'Unauthorised third party' should be defined in section 317ZG and supports the following definition:

    - A reference to any person other than:

        - the person who is the subject of the investigation by the interception agency to which the relevant TAR, TAN or TCN notice, or the person who is communicating directly with the person who is the subject of such a notice; or

        - the interception agency that issued, or requested the Attorney-General to use, the relevant TAR, TAN or TCN.

- 'Otherwise secure information' should be defined in section 317ZG and supports the following definition, subject to the insertion of 'directly or indirectly' after 'relating':

    - A reference to the information of, about or relating to any person who is not the subject, or is not communicating directly with the subject, of an investigation by the interception agency that issued, or asked for the Attorney-General to issue, the relevant TAR, TAN or TCN.

- The Act be amended to introduce a maximum time-limit after which a new TAR would have to be issued.

- Subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) be amended to include an express obligation on those seeking to extend a TAN or TCN to inform DCPs of their right to refuse the extension.

- The Act be amended so that the time-limits contained in subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) regarding the extension and variation of TANs and TCNs also apply to extension and variation of TARs.

- Sections 317HA, 317HA and 317TA be amended to include a limit on the number of fresh notices or requests that can be issued.

- Subsections 317W(7) and (8) be removed in order to eliminate the potential that a DCP may receive a 'replacement TCN' without their approval.

- The report of the assessors under subsection 317WA be binding on the Attorney-General. That is, the Attorney-General must not proceed to give a TCN if each assessor is not satisfied with the matters set out in 317WA(7).

- In section 317YA, a variation of a minor nature should only include administrative variations and substantive variations should be considered variations 'not of a minor nature'. The Supplementary Explanatory Memorandum should be amended to reflect this.

- A similar provision for assessment and report was introduced for when a DCP receives a consultation notice to vary a TCN.[8] However, the assessment and a report by two experts of whether the proposed TCN would contravene section 317ZG is available to a DCP only if the variation is 'not of a minor nature.'

- The 'reasonable and proportionate' criteria should include a broader 'less intrusive' or 'less restrictive' test than that is currently provided in the Act. The 'least intrusive' test should relate to surveillance capabilities to obtain the information through other means – not simply through industry assistance.

- The 'reasonable and proportionate' criteria be amended to:

    - include guidance on how the individual factors are to be weighed or balanced when considering whether a notice 'is reasonable and proportionate';

    - amend paragraphs 317JC(a)–(b), 317RA(a)–(b), 317ZAA(a)–(b) to include a higher threshold of 'significant or serious' national security and law enforcement interests;

    - amend paragraphs 317JC(c), 317RA(g), 317ZAA(c) to specify that the 'legitimate interests of the DCP to whom the notice relates' include commercial interests;

    - omit paragraphs 317JC(i), 317RA(g), 317ZAA(g) 'such other matters as the Director-General of Security or the chief officer, as the case requires, considers relevant';

    - insert 'or' or 'and' after each matter listed;

    - refer explicitly to the fundamental human right to privacy, or alternatively, refer to the Australian Privacy Principles under the *Privacy Act 1988* (Cth) (**Privacy Act**) and the potential privacy impact of a TAN or TCN be evidenced by a privacy impact assessment undertaken by the OAIC;

    - refer explicitly to a requirement of proportionality;

    - include factors which require the issuer of a TAR, TAN or TCN to separately consider the potential legal consequences to the recipients of warrants; and

    - require the decision maker to determine whether use of the measure is necessary in the investigation or enforcement of laws in relation to investigation or enforcement of a serious offence in circumstances where imperatives of law enforcement demonstrably outweigh reasonable expectations of confidentiality in communications of affected individuals and businesses.

- The Law Council recommends that subsection 476.2(4) of the *Criminal Code Act 1995* (Cth) (**Criminal Code**) be further amended to explicitly state that a TAR, TAN

[8] *Assistance and Access Act* s 317YA.

or TCN given no legal effect under sections 317ZG and 317ZH, and a TCN given no legal effect under section 317ZGA, will not be conferred criminal immunity.

- The Act be amended so that any issuing agency of a TAR, TAN or TCN is obliged to inform the DCP who is receiving the notice of its right to complain to the relevant overseeing or inspecting body.

- The inspection measure of the Ombudsman under section 317ZRB be amended to be a mandatory inspection power.

- The Ombudsman's terms of reference in relation to its inspection obligation under section 317ZRB expressly include the protection of privacy of individuals.

- The Act be amended so that decisions made under Schedule 1 are made by a judicial officer and not the Attorney-General, or so that a decision to issue a Schedule 1 notice must be approved by a judicial officer In the alternative, the Act be amended so that judicial review of Schedule 1 decisions under the ADJR Act is available.

- Section 317TAAA be amended so that the Minister is required to apply the decision-making criteria as contained in sections 317JAA, 317P and 317V, and consequently, be required to consider the same matters listed in sections 317JC, 317RA, 317ZAA, to ensure the issuance of the TCN is reasonable and proportionate.

- The Committee should be satisfied that the removal of the *Intelligence Services Act 2001* (Cth) (**IS Act**) from subsection 317ZH(1) would not allow for the situation where intelligence services agencies could approach issuing agencies, and vice-versa, with the intention of side-stepping a process that would otherwise require a warrant or authorisation under the IS Act.

- Section 317LA be amended to require the AFP Commissioner to not give approval for the issuance of a TAN unless satisfied of the matters specified in section 317P. In the alternative to subjecting the AFP Commissioner to decision-making criteria, section 317LA be amended to expressly state the consultative and coordination role of the AFP Commissioner.

- The Act is amended to require the Committee to undertake another review of the Act which occurs within three years from the date the review under section 187N of the TIA Act concludes.

Computer Access Warrants

- Section 32 of the SDA be amended to outline that telecommunications intercepts will not be permitted under emergency authorisations as consistent with the former subsection 32(4) of the SDA.

- Subsections 25A(4A), 27E(3A) and 27E(2A) of the ASIO Act be amended to introduce a concrete, quantifiable time-limit for the return of computers, and a requirement that the removal of a computer for any time after the prescribed time-limit must be an approved extension from a court.

- The ASIO Act and the SDA be amended to omit paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) from the ASIO Act and paragraph 27E(7)(k) from the SDA.

- Subsections 25A(9) and s 27A(3D) of the ASIO Act and subsection 27E(8) of the SDA be amended to omit the requirement that 'loss or damage' must be 'material'.

- Subsections 25A(10) and 27A(3E) in the ASIO Act and subsection 27E(9) in the SDA be amended to include a quantifiable time-limit by which a computer which has been removed in accordance with the concealment of access provisions must be returned.

- The Law Council recommends that the ASIO Act and the SDA be amended to permit disclosures about computer access warrants under Division 4 Part 2 of the SDA and under section 25A of the ASIO Act for the purpose of obtaining legal advice.

Voluntary and compulsory assistance to ASIO

Section 94 of the ASIO Act be amended to require the Director-General to include in its annual report the kinds of circumstances in which voluntary assistance (under paragraph 21A(1)(a)), and compulsory orders (under subsection 34AAA(2)), are being requested.

Ongoing Previous Law Council Recommendations

Industry Assistance Notices

- Additional resources for oversight of the activities under Schedule 1 should be made available to the relevant oversight bodies.

- Determination of listed acts or things for TCNs by legislation instrument:

    - Subsection 317T(5) be omitted. Any addition to an act or thing required under a TCN should be by way of legislative amendment.

    - In the alternative, subsection 317T(6) be amended so that considerations required by the Minister in making a determination explicitly include the potential impact on human rights, such as the right to privacy.

- Conferral of civil immunity on providers issued with a TAR, TAN or TCN:

    - Sections 317G and 317ZJ be amended:

        - to include limitations on the conferral of civil liability for providers who comply with a TAR, TAN or TCN so that civil immunity is not conferred if the conduct results in significant loss of, or damage to, property, economic loss or physical or mental harm or injury (in line with section 21A of the ASIO Act); and

        - to include limitations and exceptions, to the extent possible that reflect those available in the controlled operations scheme and appropriately modified as required for intelligence agencies.

    - In relation to ASIO, the conferral of immunity powers in relation to TARs under subsection 317G(1) of the Telecommunications Act should be by the Attorney-General.

- Appropriateness of civil and criminal immunity in relation to a TAR:

- The application of criminal immunity under subparagraph 476.2(4)(b)(iv) of the Criminal Code for TARs be limited, so that criminal immunity is only conferred in relation to acts done in accordance with a TAR.

- There should be civil indemnification rather than immunity for providers. The Commonwealth should indemnify providers who cause loss to a person or persons as a result of the provider complying with a TAR.

- Where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.

- Reporting requirements for conferral of immunities:

  - The Act should be amended to require annual reporting to the Parliament on the number of times the immunities are used; the kinds of assistance requested and provided; and the extent to which the immunity provisions did not apply.

- Accountability and oversight

  - The legislation should clearly identify the intended graduated operation of TAR, TAN and TCN powers.

  - Subsection 317ZFA(1) be amended so that a court may make an order they consider appropriate in relation to the disclosure, protection, storage, handling or destruction, the proceeding of, TAN, TCN or TAR information, if the court is satisfied that it is in the interests of justice (rather than the public interest) to make such orders.

  - When assistance has been provided under a TAR, TAN, TCN, subjects of an interception warrant or a TAR be notified of the fact once there is no prejudice to an investigation.

- For law enforcement agencies, the Act be limited to the enforcement of serious criminal laws of Australia, with the potential addition of the investigation or prosecution of serious criminal acts or omissions committed overseas where also a serious offence under Australian law. In the alternative, the relevant decision-maker must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under section 8 of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) (**MACMA**). This must be considered prior to a TAR, TAN, or TCN being given, and where the relevant purpose relates to 'assisting the enforcement of the criminal laws in force in a foreign country'.

- OAIC have direct oversight to ensure the Australian Privacy Principles under the Privacy Act are complied with be adopted.

- Consideration be given to the lack of an invasion of a privacy cause of action in Australia, in contrast to jurisdictions such as the United States.

Computer Access Warrants

- Privacy impact on third parties:
    - Paragraph 27E(2)(b) of the SDA, which authorises a computer access warrant to enter any premises for the purposes of gaining entry to, or exiting, the specified premises, be amended so that access to third party premises, computer or communication in transit should be limited to cases where an eligible Judge or nominated AAT member considers it is necessary (rather than appropriate) in the circumstances to execute the warrant, having regard to the human rights of the relevant parties including their right to privacy.
    - Paragraphs 25A(4)(aaa) and 25A(8)(e) of the ASIO Act, subparagraphs 3F(2A)(c)(i), 3F(2D)(b) and section 3F(2E) of the Crimes Act, and subparagraphs 199(4A)(c)(i) and 199B(2)(c)(i), and paragraphs 199(4C)(b) and 199B(4)(b) of the Customs Act should be subsequently be amended.
- Telecommunications interception under computer access warrant:
    - While the Law Council recognises the different features of telecommunication intercept warrants and computer access warrants, are different, in the absence of evidence to suggest why amendments to existing thresholds in relation to telecommunications interception should be lowered, the 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. This requires for example that:
        - former thresholds for ASIO a computer access warrant, foreign intelligence warrant or identified persons warrant allowing the interception of a communication passing over a telecommunications system can 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;
        - telecommunications interception under a computer access warrant should be limited to relevant offences under the SDA that are serious offences under the TIA Act; and
        - the Judge or nominated AAT member must not issue a warrant under the SDA where a control order is in force in relation to another person, and the particular person is likely to communicate with the other person using the service unless he or she is satisfied that the agency has exhausted all other practicable methods or interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible
    - The ASIO Act and the SDA should be limited to the purpose of obtaining access to 'relevant data' as defined for example under paragraphs 25A(4)(a), 25A(4)(ab), 27E(2)(c) and 27E(2)(d) of the ASIO Act and paragraphs 27E(2)(c) of the SDA.
    - In the absence of adequate justification, paragraphs 25A(5A)(a), 27A(2)(a) and 27J(3)(d) of the ASIO Act and paragraph 27E(6)(a) of the SDA be amended so that the authorisation of the use of force is prohibited for the telecommunications interception power in the new computer access warrants.

- Reporting requirements for the significantly expanded computer access warrants regime should include a requirement to report on the details of the telecommunications service to or from which each intercepted communication was made.

- 'General computer access intercept information' should be subject to the use, storage and destruction requirements in the TIA Act and SDA, rather than excluded from their operation.

- Removal of computers and other things:

    - The temporary removal power in the new computer access warrants should be limited to the purpose of obtaining access to 'relevant data' under existing paragraphs 25A(4)(a), 25A(4)(ab), 27E(2)(c) and 27E(2) (d) of the ASIO Act and paragraphs 27E(2)(c) of the SDA.

    - The criteria for what objects may be temporarily removed should be clearly set out in the legislation to ensure that there is a rational connection with the legitimate objective of the legislation.

    - There should be a requirement to aid transparency to report on all temporary removals under computer access warrants.

- Issuing of computer access warrants – law enforcement:

    - The term 'or otherwise' in paragraph 27D(1)(b)(ix) be more clearly defined.

- New section 64AD of the SDA: compulsory assistance to law enforcement relating to data:
    - Section 64AD of the SDA should clearly outline whether the 'specified person' is a natural person or a legal person.
    - The penalty available under sections 64A and 34AAA of the Act be proportionate to the penalties relating to a 'serious offence' under the Crimes Act.
    - Sections 34AAA and 64A be amended to include a 'use' immunity and a 'derivative use' immunity.

- Mutual Assistance in Criminal Matters:

    - An independent review of the MACMA should be conducted to ensure that Australia is complying with fundamental rule of law principles and its international obligations.

    - Consideration should be given to amending the MACMA to clearly define 'special circumstances' for the purposes of mutual assistance in cases where an offence in a foreign country may be punishable by the death penalty.

Voluntary assistance to ASIO

- The conferral of civil immunity powers for voluntary assistance to ASIO should be by the Attorney-General.

- Where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.

- Clarification should be provided as to the intended relationship between the immunity in section 21A of the ASIO Act and the provisions in Schedule 1 of the Acr relating to a TAR.

- The Act be amended to ensure that the immunity of civil liability does not cover conduct that causes economic loss or physical or mental harm or injury which might otherwise constitute negligence. Alternatively, it must be clear on the face of the legislation that an aggrieved person would have a legally enforceable remedy against ASIO.

- The procedural framework surrounding requests made under subsection 21A(1) and the associated immunity from civil liability should be improved in the following ways to aid transparency and accountability by making it clear:

    - that compliance with a request is voluntary (as for subsection 317HAA(1) of the Act);

    - how long the request will be in force with a maximum statutory period applying;

    - that a voluntary assistance provided to ASIO request does not cover ongoing requirements for assistance;

    - that oral requests should be followed by a written record to the person as soon as reasonably practicable;

    - the manner in which such requests may be varied or revoked; and

    - the manner in which there are reporting requirements under the provisions. There should be annual reporting to the Parliament on the number of times the provision is used; the kinds of assistance requested and provided; and the extent to which the civil immunity provision did not apply.

Compulsory assistance to ASIO

- Section 34AAA of the ASIO Act should clearly outline whether the ‘specified person’ is a natural person or a legal person.

- Subparagraph 34AAA(2)(c)(i) should require that a person is knowingly and intentionally involved in activities that are prejudicial to security.

- The legislation should make the link between the person being subject of the assistance order and the security matter explicit.

- The Explanatory Memorandum should explain why only computers and storage devices not on the premises are subject to 34AAA(3).

- Section 34AAA should include adequate record keeping requirements, reporting requirements, instructions for the cessation of activities and destruction of materials at least consistent with other parts of the ASIO Act.

- Informing the person of the order:

    - A person should be notified directly that an order exists with information including a specified time period.

- Complying with the order amounting to detention:
    - The Act should be amended to as a minimum:
        - allow the person to contact a lawyer or family member, where in the former case client confidentiality is preserved;
        - prescribe a maximum period for the giving of assistance;
        - require officers to explain the nature of the order, complaint mechanisms of the IGIS/Commonwealth Ombudsman or how to challenge the order in a court;
        - require an interpreter if necessary;
        - require that the person is treated humanely and with respect for their human dignity;
        - require, at the very least, for the person to be brought before a Federal Court Judge for a hearing in camera after 4 hours have elapsed to enable an application for release or extension of time period as per for example existing provisions for the arrest and interview of suspects under the Crimes Act.
- Questioning and detention warrants:
    - There should be requirements to guard against oppressive use of multiple coercive powers to obtain particular information.

Key Issues

Schedule 1 - Industry Assistance Notices

'Listed acts or things'

'Serious offences'

11. The industry assistance measures under Schedule 1 of the Act apply to the investigation and prosecution of 'serious Australian offences' and 'serious foreign offences'. These terms were introduced to the Act by the Government amendments.

12. The Government amendments omitted from subparagraph 317E(1)(j)(i) the words 'and laws imposing pecuniary penalties' and replaced them with 'so far as it relates to serious Australian offences'. Subparagraph 317E(1)(j)(ii) was also amended to insert 'so far as those laws relate to serious foreign offences'.

13. The Government amendments inserted in the Act a definition of 'serious Australian offence' and 'serious foreign offence':

> ***serious Australian offence*** *means an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more or for life.*
>
> ***serious foreign offence means*** *an offence against a law in force in a foreign country that is punishable by a maximum term of imprisonment of 3 years or more or for life.*[9]

14. The effect of these amendments it that the powers set out in Schedule 1 of the Act, in particular, the power to give a TAR, TAN or TCN[10] can be used against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more, or for life.

15. This amendment appears consistent with the Committee's recommendation from its Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**report on the Bill**) that:

> *the industry assistance measures under Schedule 1 of the Telecommunications (Assistance and Access) Bill 2018, so far as they relate to criminal law enforcement, apply to offences with a penalty of a maximum period of three year's imprisonment or more*.[11]

16. The Supplementary Explanatory Memorandum states that the application of Schedule 1 powers regarding industry assistance to 'serious offences' is a reasonable and proportionate interference with the right to privacy:

> *These definitions further clarify that the exercise of powers in Schedule 1 are a permissible limitation to the right to privacy as they are reserved for serious offences including terrorism and child exploitation offences. Invoking the powers in Schedule*

[9] Ibid s 317B definition of 'serious Australian offence' and 'serious foreign offence'.
[10] Ibid ss 317G, 317L, 317T.
[11] 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, ix [2.3].

1 is a reasonable and proportionate interference with the right to privacy given the nature of the offences under investigation.[12]

17. The Schedule 1 powers under the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**the Bill**) were intended to target the enforcement of offences relating to terrorism or child exploitation.[13] The Law Council considers that the definition of 'serious offences' should be equivalent of the definition of 'serious offences' under the TIA Act.[14]

18. Broadly, an offence is a 'serious offences' under subsection 5D(1) of the TIA Act if it is:

    (a) murder;[15]

    (b) kidnapping;[16]

    (c) a drug offence under Division 307 of the Criminal Code;[17]

    (d) an offence constituted by conduct involving an act of terrorism,[18] including the offence of advocating terrorism, terrorism offences under sections 101-103 of the Criminal Code, the offence of contravening a control order and offences foreign incursions and recruitment;[19]

    (e) an explosives and lethal devices offence under Division 72 of the Criminal Code;[20]

    (f) a treason or urging violence offence under Division 80 of the Criminal Code;[21] or

    (g) a national security offence, such as sabotage, espionage, foreign interference, theft of trade secrets involving foreign government principal;[22]

19. In addition, an offence is a 'serious offences' under subsection 5D(1) of the TIA if:

    (a) it is an offence punishable by imprisonment for life or for a period of at least seven years; and

    (b) the particular conduct constituting the offence involved, involves, or would involve:

        (i) loss of a person's life, or risk of;

        (ii) serious personal injury, or risk of;

[12] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 7 [7].
[13] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 2 [4].
[14] *Telecommunications (Interception and Access) Act 1979* (Cth) s 5D.
[15] Ibid s 5D(1)(a).
[16] Ibid s 5D(1)(b).
[17] Ibid s 5D(1)(c).
[18] Ibid s 5D(1)(d).
[19] Ibid s 5D(1)(e)(ib), (ii)–(vi).
[20] Ibid s 5D(1)(e)(i).
[21] Ibid s 5D(1)(e)(ia).
[22] Ibid s 5D(1)(e)(ic), (ie), (if), (ig).

(iii) serious damage to property in circumstances endangering the safety of a person;

(iv) serious arson;

(v) trafficking in prescribed circumstances;

(vi) serious fraud;

(vii) serious loss of revenue of the Commonwealth, a State or the ACT; or

(viii) bribery or corruption by public officials.[23]

20. Subsections 5D(3)–(9) of the TIA provide for further offences which constitute 'serious offences', including offences which relate to:

(a) offences involving planning and organisation;

(b) offences relating to criminal groups;

(c) offences relating to smuggling, slavery sexual servitude, deceptive recruiting and trafficking in persons;

(d) sexual offences against children and offences involving child pornography or harm to children;

(e) money laundering offences;

(f) cybercrime offences;

(g) serious drug offences;

(h) cartel offences;

(i) market misconduct;

(j) offences connected with other serious offences; and

(k) offences relating to criminal organisations.

21. The Law Council considers that by setting the bar at offences which carry a penalty of imprisonment of three years or more, the threshold for the application of the powers in Schedule 1 of the Act is too low. The current definition sets a very broad scope, as they could be used, in theory, to could capture individuals suspected of committing relatively minor criminal offences, such as theft.

22. The Law Council does not support the definition of 'serious Australian offences' and 'serious foreign offences' as introduced by the Government amendments. The Law Council recommends that the definition of 'serious offences' should be consistent with the TIA in so far that 'serious offences' is defined as laws of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of seven years or more, rather than three years.

[23] Ibid s 5D(2).

Exhaustive list of 'listed acts or things'

23. In the Bill, subsections 317G(6), 317L(3) and 317T(7) provided that an act or thing stated in a TAR, TAN or TCN includes, but is not limited to, listed acts or things under section 317E. This meant that the listed acts or things that could be required under a TAR or TAN were non-exhaustive.

24. In the Law Council's submission to the Committee's inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**previous submission**), it recommended that the listed acts or things under section 317E remain exhaustive for TARs, TANs and TCNs by removing the words '(but are not limited to)' under subsections 317G(6), 317L(3) and 317T(7).

25. The Committee also recommended in its report on the Bill that the definition of 'listed acts or things' be exhaustive.'[24]

26. The Government amendments replaced the words '(but are not limited to)' with 'must be' in subsections 317L(3) and 317T(7), rendering the listed acts or things under section 317E for TANs and TCNs exhaustive. This ensures that acts or things for the purpose of a TAN or TCN are all present in section 317E. However, the words '(but are not limited to)' remain in subsection 317G(6). As such, the listed acts or things under section 317E for TARs remain non-exhaustive.

27. It appears the Government amendments are only partly consistent with the Law Council's recommendation, as the listed acts under section 317E for TARs are not exhaustive. There is nothing provided in the Supplementary Explanatory Memorandum to explain why the Government amendments addressed this issue in relation to TANs and TCNs, but not for TARs. The Law Council recommends that subsection 317G(6) is amended to replace the words '(but are not limited to)' with 'must be', as was done for subsections 317L(3) and 317T(7).

'Giving help'

28. Subsection 317L(2A) has been introduced by the Government amendments to make it clear that TANs must not used to require DCP to build new capabilities. The Law Council supports this additional paragraph to the acts or things that a DCP may be required to comply with under a TAN, as it makes clear that a TAN must not be directed towards ensuring that a DCP is capable of giving help to ASIO or an interception agency.

Unauthorised disclosure of information

29. Subsection 317ZF(1) was introduced by the Bill, which creates a secrecy offence for disclosures of information relating to TARs, TANs and TCNs. Subsection 317ZF(3) provides exceptions to this offence, providing instances in which the persons listed in paragraph 317ZF(1)(b) may disclose TAR, TAN or TCN information. It is positive step that the Government amendments to the Act added that disclosure to 'an Ombudsman official for the purpose of exercising powers, or performing functions, or duties, as an Ombudsman official' is an 'authorised disclosure'. [25]

[24] 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, xi [2.11].
[25] *Assistance and Access Act* s 317ZF(5A).

30. However, the Law Council maintains its position that disclosure of TAR, TAN or TCN information to the OAIC and ACLEI should also be 'authorised disclosures' under section 317ZF(3),[26] as is provided for in paragraphs 122.5(3)(iia) and (iii) of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 201*8 (Cth) (**EFI Act**). Furthermore, the Act should be amended to provide for a defence to the unauthorised disclosure of information in accordance with the Public Interest Disclosure Act 2013 (Cth) (**PID Act**) or the *Freedom of Information Act 1982* (Cth) (**FOI Act**), unlike the EFI Act.[27]

31. Another improvement to section 317ZF by the Government amendments is the expansion of the instances in which disclosure of information regarding TARs, TANs and TCNs is 'authorised' under section 317ZF. First, disclosure to a State or Territory inspecting body has been added to section 317ZF as an 'authorised disclosure'.[28] The Act provides that information relating to a TAR, TAN or TCN may be disclosed to an officer or employee of an authority of the State or Territory inspecting agency in relation to the interception agency by:

    (a) the Ombudsman, in relation to a TAR or TAN given by the officer of an interception agency of a State;[29]

    (b) the Communications Access Co-ordinator, in relation to a TCN given by the Attorney-General;[30] or

    (c) a DCP, an employee of a DCP, a contracted service provider of the DCP (**CSP**) or an employee of a CSP, in relation to a TAR or TAN given the chief officer of an interception agency of a State or Territory;[31]

    so long as disclosure if in connection with the officer or employee exercising powers, or performing functions or duties.

32. It appears that this amendment is consistent with the Committee's recommendation in its report on the Bill that the Act include 'express notification requirements and information sharing provisions which would complement the inspection activities of State and Territory oversight bodies.'[32]

33. Secondly, the amendments introduced subsections 317ZF(14)–(16), which allow for a DCP, CSP, or a specified employee of a DCP or CSP, to 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 that has been given by the Director-General of Security or by the chief officer of an interception agency,[33] or to the Attorney-General in relation to a TCN that has been given by the Attorney-General.[34] If a request

---

[26] 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, 32-3 [92]-[98].
[27] *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Cth)* s 122.5(4).
[28] *Assistance and Access Act* ss 317ZF(5B)–(5C).
[29] Ibid s 317ZF(5B)–(5C), (12A)–(12D).
[30] Ibid s (12A).
[31] Ibid ss 317ZF(12B)–(12C)
[32] 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, x [2.6].
[33] *Assistance and Access Act* ss 317ZF(14)–(15).
[34] Ibid ss 317ZF(16).

for disclosure is authorised, the disclosure must be in accordance with the conditions (if any) specified in the authorisation.

34. The Committee recommended in its report on the Bill that:

> *the Bill 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*.[35]

35. These amendments improve the unauthorised disclosure provisions as contained in the Bill. However, the Law Council considers that the additions made to section 317ZF by the Government amendments 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.

36. For example, for a DCP or an employee of a DCP to disclose information to an individual or body not provided for in subsections 317ZF(1)–(13) without committing an offence under subsection 317ZF(1), the DCP or employee must make a request for authorisation under subsections 317ZG(14)–(16), which must be granted by the relevant agency. The Act grants broad discretionary powers to the Director-General of Security, the chief officer of an interception and the Attorney-General, regarding the decision of whether to grant a request for authorised disclosure, as the Act does not provide any indication of the circumstances in which an information disclosure request should or should not be authorised.

37. As such, the Law Council supports the proposed amendment 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.[36] This would be consistent with the Committee's recommendation in its report on the Bill.[37]

38. Furthermore, the Law Council consider this particularly concerning since the Act does not provide for a defence to the unauthorised disclosure of information in accordance with the PID Act or the FOI Act. If a DCP, or an employee of a DCP, disclosed information relating to a TAR, TAN or TCN to an individual or body not provided for in subsections 317ZF(1)–(13), and without authorisation under subsections 317ZF(14)–(16), the employee would have committed an offence under subsection 317ZF(1), which carries the penalty of five years imprisonments. The DCP, or the employee, would not have available to it the defence, for example, that the disclosure was in the public interest. Furthermore, the Law Council considers that criminal sanctions for the disclosure of information should only be used when strictly required for the effective functioning of government.[38]

---

[35] 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].
[36] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8625 proposed amendment (7).
[37] 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].
[38] Law Council of Australia, Submission to the Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, 27 February 2009, [3]-[4].

39. In addition, the Law Council maintains its position that the secrecy offence in subsection 317ZF(1) should include an express harm requirement.[39]

Statutory review

40. The Government amendments require the Committee to review of the operation of the amendments made by the Act. Section 187N of the TIA Act was inserted by the Government amendment to require the Committee to review the amendments made by the Act within the same timeframes as the compulsory review of Part 5-1A of the TIA Act. This means the Committee must commence its review of Part 5-1A of the TIA Act and the amendments made by the Act by 13 April 2019 and must conclude its review by 13 April 2020.

41. The Law Council supports review of the Act by the Committee, as the Committee's robust review is an important public accountability and transparency measure. However, the Law Council considers that it is not clear how the current review by the Committee relates to the review required by section 187N of the TIA Act. The Committee must release its report from its current review by 3 April 2019, yet is also required to have commenced its review under section 187N of the TIA Act just ten days later.

42. Furthermore, the effect of 187N for the TIA Act is that it requires the Committee to conclude its review before the end of the Act's 18-month implementation period.

43. The Law Council recommends that the Act is amended to require the Committee to undertake another review of the Act which occurs within three years from the date the review under section 187N concludes.

44. In addition, the Government amendments to the Act inserted subsection 6(2) to the *Independent National Security Legislation Monitor Act 2010* (Cth). This section requires the INSLM to review the operation, effectiveness and implication of the amendments made by the Act, 18-months after 8 December 2018.

45. This recommendation is consistent with the Committee's recommendation in its report on the Bill.[40] The Law Council recognises the critical role that the INSLM has in the expert review of laws relating to national security. The Law Council supports an INSLM review of the Act as it is an important step to achieving appropriate oversight of the measures introduced by the Act.

'Systemic weakness' and 'systemic vulnerability'

46. Subsection 317ZG(1) provides that a TAR, TAN or TCN must not have the effect of:

    (a) requesting or requiring a DCP to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or

    (b) preventing a DCP from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.[41]

---

[39] 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, 32-3 [93]-[96].
[40] 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 [2.15].
[41] *Assistance and Access Act* s 317ZG(1).

47. The Government amendments introduced a non-exhaustive definition of 'electronic protection' into the Act.[42] 'Electronic protection' includes authentication and encryption. The Supplementary Explanatory Memorandum states that the purpose of the definition is:

> *to clarify those technologies which must not be undermined as they are critical to protecting the security of personal information*.[43]

Application to TARs

48. In the Law Council's previous submission, it noted that section 317ZG would have prohibited a TAN or TCN from requiring DCP to introduce a 'systemic weakness' or 'systemic vulnerability' into a form of electronic protection, but there was no such protection for TARs.[44]

49. The Law Council is pleased that the Government amendments to the Act addressed this issue through the amendment of subsection 317ZG(1) to broaden its scope to include TARs.

50. This amendment is consistent with the Committee's recommendation in its report on the Bill.[45]

Definition of 'systemic weakness' and 'systemic vulnerability'

51. In the Law Council's previous submission, it stated that there appeared to be ambiguity in what may constitute a 'systemic weakness' and 'systemic vulnerability'.[46]

52. The Law Council notes that the Government introduced a definition of 'systemic weakness' and 'systemic vulnerability':

> ***systemic vulnerability*** *means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*
>
> ***systemic weakness*** *means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.*[47]

53. However, the Law Council does not support the proposed definitions of 'systemic weakness' and 'systemic vulnerability' on the basis that they simply allow for the introduction of any weakness or vulnerability as requested. The Law Council considers that the definitions have the potential to make it a very vague and high standard to meet

---

[42] Ibid s 317B definition of 'electronic protection'.
[43] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 10 [11].
[44] 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*,* 18 [27].
[45] 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, xiv [2.18].
[46] 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*,* 18 [27].
[47] *Assistance and Access Act* s 318B definition of 'systemic weakness' and 'systemic vulnerability'.

before planned intervention can be said to be appropriate in a given scenario. Given that their very intention is to introduce a diminution in security standards, the working combination of these new definitions remains a concern.

54. The term 'whole class of technology' is not defined in the Act. The Supplementary Explanatory Memorandum provides some explanation regarding the intended meaning of 'whole class of technology.' It states that the 'systemic weakness' and 'systemic vulnerability' definitions:

> *mak[e] clear that a systemic weakness is something that makes general items of technology less secure. Technological classes include particular mobile device models carriage services, electronic services or software. The term is intended to encompass both old and new technology or a subclass within a broader class of technology; for example an iOS mobile operating system within a particular class, or classes, of mobile devices*.[48]

55. The term 'target technology' is defined in the Act.[49] The definition provides that:

(a) a particular carriage service, so far as the service is used, or is likely to be used, (whether directly or indirectly) by a particular person, is a target technology that is associated with that person;

(b) a particular electronic service, so far as the service is used, or is likely to be used, (whether directly or indirectly) by a particular person, is a target technology that is associated with that person;

(c) particular software installed, or to be installed, on a particular computer or a particular item of equipment, used, (whether directly or indirectly) or likely to be used, by a particular person is a target technology that is associated with that person;

(d) a particular update of software that has been installed on a particular computer or a particular item of equipment that is used, (whether directly or indirectly) or likely to be used, by a particular person is a target technology that is associated with that person;

(e) a particular item of customer equipment used, or likely to be used, (whether directly or indirectly) by a particular person is a target technology that is associated with that person; and

(f) a particular data processing device used, or likely to be used, (whether directly or indirectly) by a particular person is a target technology that is associated with that person.[50]

56. The Supplementary Explanatory Memorandum states the intended operation of subsection 317ZG(1):

> *while systemic weaknesses or vulnerabilities cannot be built into services or devices, a technical assistance notice can require the selective introduction of a*

[48] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 15 [51].
[49] *Assistance and Access Act* s 317B definition of 'target technology'.
[50] Ibid s 317B definition of 'target technology'.

> *weakness or vulnerability in a particular service, device or item or software on a case-by-case basis*.[51]

57. In the Law Council's previous submission, it recommended that subsection 317ZG(1) be amended so that 'electronic protection' be replaced by 'current or proposed product or service'.[52] It expressed concerns that although a provider cannot be required to 'implement' or 'build' new capabilities to remove electronic protections, providers could be required to install software or hardware that is subject to a backdoor or other vulnerability. Alternatively, providers could be required to modify or place limitations on proposed, unreleased products or services. A TAR, TAN or TCN could also require a provider to modify or substitute a service to remove other features that prevent decryption or provide some other security benefit.[53]

58. It appears that the Law Council's concerns remain. It appears that subsection 317ZG(1) would operate to allow TARs, TANs and TCNs to introduce a weakness or a vulnerability into software or hardware[54] and carriage and electronic services.[55] Requirements which permit the weakening of a form of electronic protection are expressly permissible when the electronic protection is 'connected' to a person of interest. The Act does not provide a definition or explanation of 'connected'. The Supplementary Explanatory Memorandum provides some explanation on the intended meaning of 'connected':

> *The term 'connected' is intended to capture technologies associated with the particular person and reflects the modern use of communications devices and services. It is narrower than the broader notion of 'connectivity' with the internet*.[56]

59. The Law Council's concerns with respect to the use of the term 'connected' is that it casts the net of technologies and their uses by individuals, which may be vulnerable to the introduction of a weakness or vulnerability, very wide. The Law Council is unsure as to how the term 'connected' in the Act could be interpreted to be narrower than the notion of 'connectivity' with the internet, as the Supplementary Explanatory Memorandum claims, without any explanation of the term included within the Act.

60. The Law Council maintains its position that the Act be amended to prohibit a TAR, TAN or TCN from requesting or requiring *any* act or omission that might require a DCP to either implement or build *any* weakness or vulnerability into a current or proposed product or service.

61. In the alternative, if the current definitions of 'systemic weakness' and 'systemic vulnerability' remain in the Act, the Law Council submits that terms 'whole class of technology' and 'connected' be defined in the Act. The Law Council regards the meaning of key term 'whole class of technology' as unclear and uncertain. As mentioned above, the term 'whole class of technology' is not defined. This may make it difficult to interpret and introduce uncertainty. For the rule of law to be upheld, it must be both readily known and available, and certain and clear, which includes the requirement that key terms should be defined.[57]

---

[51] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 16-7 [55].
[52] 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*,* 18 [26].
[53] Ibid.
[54] *Assistance and Access Act* s 317B definition of 'target technology (c), (d)'.
[55] Ibid s 317B definition of 'target technology (a), (b)'.
[56] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 16 [52].
[57] Law Council of Australia, Policy Statement on Rule of Law Principles (March 2011), 2 Principle 1(b).

Safeguards to protect against unauthorised third-party access

62. The Government amendments inserted subsections 317ZG(4A) and (4B) to clarify that, in a case where a weakness or vulnerability is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph 317ZG(1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person. Subsection 317ZG(4C) provides that for the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.

63. The Law Council holds the view that clarity and certainty should be added to the safeguards. The Law Council supports the proposed amendment to section 317ZH that 'unauthorised third party' should be defined in section 317ZG and supports the following definition:

> *A reference to any person other than:*
>
> *the person who is the subject of the investigation by the interception agency to which the relevant TAR, TAN or TCN notice, or the person who is communicating directly with the person who is the subject of such a notice; or*
>
> *the interception agency that issued, or requested the Attorney-General to use, the relevant TAR, TAN or TCN*.[58]

64. The Law Council supports the proposed amendment that 'otherwise secure information' should be defined in section 317ZG and notes the following proposed definition:

> *A reference to the information of, about or relating to any person who is not the subject, or is not communicating directly with the subject, of an investigation by the interception agency that issued, or asked for the Attorney-General to issue, the relevant TAR, TAN or TCN*.[59]

65. The Law Council supports this proposed definition subject to further clarity being provided through the express inclusion that 'otherwise secure information' is information that is directly or indirectly, of, about or relating to, any person who is not the subject of a TAR, TAN or TCN.

Duration of TARs, TANs and TCNs

66. The Government amendments introduced a maximum time-limit for the operation of all TANs and TCNs under subsections 317MA(1A) and 317TA(1A).[60] This ensures that TANs and TCNs cannot be in effect for longer than 12 months. The Law Council supports the introduction of this time-limit. This amendment appears to be consistent

[58] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8626 proposed amendment (1).
[59] Ibid.
[60] *Assistance and Access Act* ss 317MA(1A), 317TA(1A).

with the recommendation of the Committee in report on the Bill that TANs and TCNs be subject to statutory time-limits.[61]

67. However, the Government amendments did not introduce a time-limit for the operation of TARs. Therefore, the Government amendments relating to time-limits is only party consistent with the Law Council's recommendation that a maximum-time limit apply to all Schedule 1 notices. The Law Council maintains its recommendation from its previous submission that the Act be amended to introduce a maximum time-limit after which a new TAR, TAN or TCN would have to be issued.[62]

68. The Government amendments introduced a measure to extend the life of a notice past the 12-month limitation. Under subsections 317MA(1C)–(1D) and 317TA(1C)–(1D), with the agreement from the DCP, a TAN or TCN can be extended for a further period (not exceeding 12 months) or further periods (not exceeding 12 months in each case) the period for which the TAN or TCN is in place.[63] Subsections 317Q(11) and 317X(5) require that a variation of a TAN or TCN must not extend the period for which the notice is in force. This amendment appears consistent with the Committee's recommendation in its report on the Bill that any extension or variation of TANs and TCNs be subject to statutory time-limits.[64]

69. However, this amendment is not consistent with the Law Council's recommendation in its previous submission because the time-limits on the extension and variation of TANs and TCNs have not been applied to TARs. The Law Council recommends that the Act be amended so that the time-limits as contained in subsections 317MA(1C)–(1D), 317TA(1C)–(1D), 317Q(11) and 317X(5) also apply to the extension and variation of TARs.

70. Furthermore, it appears that the Government amendments have not adopted the Law Council previous recommendation that sections 317HA, 317HA and 317TA include a limit on the number of fresh notices or requests that can be issued. As such, the Law Council maintains its recommendation that the extension provisions place a limit on the number of fresh notices that can be issued.

71. As noted above, the extension of a TAN or TCN requires the agreement of the DCP.[65] The Act must make it expressly clear that a notice can only be extended with the agreement of DCPs and not otherwise. There should be requirements placed on interception agencies to inform DCPs that they can refuse a request for extension of a TAN or TCN, particularly at the point when a request for extension is on foot.

72. In the Law Council's previous submission, it recommended that the Act be amended to include a periodic review stage of a TAR, TAN or TCN to assist oversight and accountability agencies.[66] If an interception agency seeks to extend a TAN or TCN, and the DCP does not consent to the extension, the interception agency would be required

---

[61] 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, x [2.7].
[62] 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*,* 20-1 [35]-[40].
[63] *Assistance and Access Act* ss 317MA(1C)–(1D), 317TA(1C)–(1D).
[64] 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, x [2.7].
[65] *Assistance and Access Act* ss 317MA(1C)–(1D), 317TA(1C)–(1D).
[66] 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*,* 20-1 [40].

to issue a new TAN or TCN in accordance with the procedures under the Act. This means that the interception agency would be required to evaluate the reasonableness and proportionality of a TAN or TCN every 12 months. Considering the absence of a requirement for review of a TAN or TCN, it is particularly important that DCPs have knowledge of their right to refuse an extension and interception agencies actively inform DCPs of this right.

73. The Law Council recommends that subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) be amended to include an express obligation on issuing agencies seeking to extend a TAR, TAN or TCN to inform DCPs of their right to refuse the extension.

Consultation requirements

74. The Government amendments introduced section 317PA, requiring the Director-General of Security or the chief officer of an interception agency to consult with the DCP prior to the issuing of a TAN.[67] The Director-General of Security or the chief officer of an interception agency are not required to consult with a DCP prior to issuing a TAN if satisfied that the TAN should be given as a matter of urgency, or if the DCP has waived the duty to consult.[68]

75. There are more stringent consultation requirements imposed on the decision-maker when issuing a TCN. Subsection 317W(1) requires the Attorney-General to give a DCP a written notice which sets out the proposal to give a TCN and invites the DCP to make a submission to the Attorney-General on the proposed TCN. The Attorney-General must consider the DCP's submission it if was provided within 28 days. This requirement also applies when the Attorney-General seeks to vary a TCN.[69]

76. The Supplementary Explanatory Memorandum states that:

> *The purpose of this amendment is to ensure providers are afforded an opportunity to challenge the requirements in a notice if they believe it may lead to the introduction of a systemic weakness or vulnerability or if the requirements are not reasonable or proportionate. This is an important measure as it ensures that the requirements in a proposed notice are altered before the notice is issued in order to prevent those systems which maintain the security of personal information from being undermined.*[70]

77. However, subsection 317W(7) was inserted by the Government amendments to provide that subsection 317W(1) does not apply to a TCN to be given to a DCP if the TCN is a 'replacement TCN'. That is, if the requirements imposed by the proposed TCN are the same, or substantially the same, as the requirements imposed by another TCN that has previously been given to the provider and the proposed TCN is to come into force immediately after the expiry of the other TCN, the DCP is not given a written notice.

78. Subsection 317W(8) was inserted by the Government amendments to provide that before a DCP is given a TCN, whereby the requirements of which are the same or substantially the same as the requirements imposed by another TCN previously given to the provider, and the first-mentioned TCN is to come into force immediately after the expiry of the other TCN, the Attorney-General must consult the provider.

---

[67] *Assistance and Access Act* s 317PA(1).
[68] Ibid s 317PA(2)–(3).
[69] Ibid s 317XA.
[70] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 10 [11].

79. It appears that the effect of subsections 317W(7) and (8) is that when a proposed TCN has substantially the same requirements as a TCN that is currently in place, and is expected to commence immediately after the expiry of the TCN which is currently in operation, the Attorney-General is not required to provide the DCP with a written notice and the DCP is not afforded the opportunity to make a submission to the Attorney-General. Instead, the only requirement on the Attorney-General is that it consult with DCP.

80. Under subsection 317TA(1), the extension of a TCN can occur only with the agreement of the DCP. Whereas, it appears that under subsections 317W(7) and (8), there is the potential for a 'replacement' TCN, which has the same or substantially the same requirements as an existing TCN given to the provider, to be given to a DCP without their agreement, and without the opportunity to submit in writing their views or concerns regarding the TCN to the Attorney-General. Essentially, while a TCN can only be 'extended' with the agreement of the DCP, it seems that a DCP cannot refuse the imposition of a 'replacement' TCN that has the same or substantially the same requirements as a current TCN. The effect of subsections 317W(7) and (8) is that it could allow for a replacement TCN,which effectively has the same requirements as a previous TCN, be given to a DCP without its consent..

81. The Law Council considers that the threshold in subsections 317W(7) and (8) of 'substantially the same' appears to be low. Further, there appears to be ambiguity in what may constitute 'substantially the same' TCN requirements.

82. The Law Council recommends that subsections 317W(7) and (8) be removed in order to eliminate the potential that a DCP may receive a 'replacement TCN' without their approval. If a TCN is to cease, for example at the end of a 12-month period due to the new limitations introduced by the Government amendments, and the issuing agency seeks to have that TCN continue, subsections 317W(7) and (8) should not be used to side-step the consent of a DCP to the extension of a TCN. The Law Council considers that the issuing agency must be required to obtain the consent for the extension of a TCN. If consent is not provided for the extension of the TCN, the issuing agency must be required to issue a new TCN, in accordance with the procedures and safeguards for proportionality and reasonableness as provided under the Act, regardless of how different or similar the requirements of the new TCN are compared to the requirements of a previous TCN.

Assessment by experts for TCNs

83. The Government amendments introduced subsection 317WA(1) to allow for a DCP, who has been given a consultation notice in relation to a proposed TCN, to give the Attorney-General a written request for an assessment of whether the TCN should be given. The Attorney-General must appoint two assessors:

    (a) one person who has knowledge that would enable the person to assess whether proposed technical capability notices would contravene section 317ZG and is cleared for security purposes to the highest level required by staff members of ASIO or such lower level as the Attorney-General approves;[71] and

    (b) one person who has served as a judge in one or more prescribed courts for a period of 5 years and a person who no longer holds a commission as a judge of a prescribed court.[72]

[71] *Assistance and Access Act* s 317WA(4).
[72] Ibid s 317WA(5).

84. The assessors must carry out an assessment of whether the notice should be given. In making their assessment, the assessors must consider whether:

    (a) the proposed technical capability notice would contravene section 317ZG (the prohibition against systemic weaknesses);

    (b) the requirements imposed by the proposed notice are reasonable and proportionate;

    (c) compliance with the proposed notice is practicable;

    (d) compliance with the proposed notice is technically feasible; and

    (e) it is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed notice.[73]

85. The assessors must give the most weight to whether the proposed technical capability notice would contravene section 317ZG. The assessors must prepare a report and give that report to the relevant parties.[74]

86. Section 317WA is consistent the recommendation in the Committee's report on the Bill.[75] It also adds some further safeguards, such as the duty to consult with the DCP, as well as ASIO or the chief officer of the interception agency, and the provision that the report must be considered by the Attorney-General in its consideration whether to proceed in giving the TCN.[76]

87. In the Law Council's previous submission, it recommended that the Bill be amended so that decisions made under Schedule 1 are made by a judicial officer and not the Attorney-General.[77] As such, it considers that the requirement that the Attorney-General consider the report, written by an expert and former judge in its consideration of whether to proceed to give a TCN, is not sufficient.

88. In order to ensure that this added layer of review and assessment of whether an TCN should be issued is objective and brings an external perspective to the decision-making, the Law Council supports the proposed amendment that the report of the assessors be binding on the Attorney-General. That is, the Attorney-General must not proceed to give a TCN if each assessor is not satisfied with the matters set out in 317WA(7).[78]

89. A similar provision for assessment and report was introduced for when a DCP receives a consultation notice to vary a TCN.[79] However, the assessment and a report by two experts of whether the proposed TCN would contravene section 317ZG is available to a DCP only if the variation is 'not of a minor nature.'

---

[73] *Assistance and Access Act* s 317WA(7).
[74] Ibid s 317WA(6).
[75] 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, xi-xii [2.12].
[76] *Assistance and Access Act* s 317WA(11).
[77] 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*,* 21-2 [41]-[45], 31-2 [86]-[91].
[78] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8625 proposed amendment (4), (6).
[79] *Assistance and Access Act* s 317YA.

90. The Law Council recommends that a variation 'of a minor nature' should only include administrative variations and substantives variations should be considered variations 'not of a minor nature'. The Supplementary Explanatory Memorandum should be amended to reflect this.

Decision-making criteria

91. In the Law Council's previous submission, it noted that the Bill contained far more limited decision-making criteria for the issuance of a TAR than the decision-making criteria for a TAN or TCN.[80] The Law Council supports the Government's insertion of subsection 317JAA(1) which requires that the issuance of a TAR must be reasonable and proportionate, and compliance with the request is practicable and technically feasible.[81] The effect of this amendment is that decision-making requirements apply to all Schedule 1 industry assistance notices.

92. The Law Council welcomes the Government amendment which introduced the application of decision-making criteria to the variation of TARs, TANs and TCNs.[82]

93. The Law Council supports the Government amendment which makes clear that if a TAR, TAN or TCN is not reasonable or proportionate, or the compliance with the request is not practicable or technically feasible, the notice must be revoked.[83]

94. The Law Council supports the Government's addition of 'necessity' to the list of matters which must be considered when deciding whether the requirements imposed by a TAR, TAN or TCN are reasonable and proportionate.[84] However, it considers that an express requirement of proportionality must be added to the decision-making criteria.

95. The Supplementary Explanatory Memorandum states that the inclusion of a 'necessity' factor:

> *provides confidence that, under the oversight of the decision-maker, any limitation to the right of privacy under a compulsory notice in Schedule 1 of the Bill is permissible as being necessary to ensure national security and public order*.[85]

96. The Government amendments added a 'least intrusive' requirement the list of matters which must be considered when deciding whether the requirements imposed by a TAR, TAN or TCN are reasonable and proportionate. New paragraph 317RA(ea) provides that in considering whether the requirements imposed by a TAR, TAN or TCN are reasonable and proportionate, the decision-maker must have regard to whether the requirements of the notice, when compared to other forms of industry assistance known to the decision-maker, are the least intrusive form of industry assistance as far as a person whose activities are not of interest to ASIO or the interception agency (for TARs, TANs and TCNs),[86] or of interest to the Australian Secret Intelligence Service or the Australian Signals Directorate (TARs only),[87] are concerned.

---

[80] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 s 317G(1)(a)(v)–317(1)(a)(v).
[81] *Assistance and Access Act* s 317JAA.
[82] Ibid ss 317JA(9)–(14), 317Q(10), 317X(4).
[83] Ibid ss 317JB(1A)–(3A), 317R, 317Z.
[84] Ibid ss 317JC(g), 317RA(eb), 317ZAA(eb).
[85] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 10 [11].
[86] *Assistance and Access Act* ss 317RA(ea)(i)–(ii), 317ZAA(ea)(i)–(ii).
[87] Ibid s 317JC(f).

97. The Supplementary Explanatory Memorandum provides that the requirement for decision-makers to consider if the requirements under a TAR, TAN or TCN are the least intrusive known form of industry assistance when compared to other forms of industry assistance in relation to the impact on the privacy of innocent third parties further limits the ability of Schedule 1 powers being used to arbitrarily or unlawfully interfere with the privacy of innocent parties.[88]

98. This 'least intrusive' test is significantly different from a 'least intrusive' or 'least restrictive' test in other contexts, such as for high-risk terrorist offenders in paragraph 105A.12(4)(b) of the Criminal Code.

99. The 'least restrictive' test provided for in paragraph 105A.12(4)(b) of the Criminal Code requires a court to affirm a detention order for a terrorist offender if 'satisfied that there is no other less restrictive measure that would be effective in preventing the unacceptable risk.'[89] This is a broad 'less restrictive' test which requires a court to consider all other measures which could be effective in preventing the unacceptable risk that the terrorist offender poses.

100. The Law Council recommends that the 'reasonable and proportionate' criteria should include a broader 'less intrusive' or 'less restrictive' test than that is currently provided in the Act. The Law Council considers that the 'least intrusive' test should relate to surveillance capabilities to obtain the information through other means – not simply through industry assistance.

101. The Law Council notes that the recommendations relating to the 'reasonable and proportionate' criteria contained in its previous submission were not included in the Government amendments. The Law Council considers that there are outstanding issues relating to the 'reasonable and proportionate' criteria and recommends that Act be amended to:

(a) include guidance on how the individual factors are to be weighed or balanced when considering whether a notice 'is reasonable and proportionate';

(b) amend paragraphs 317JC(a)–(b), 317RA(a)–(b), 317ZAA(a)–(b) to include a higher threshold of 'significant or serious' national security and law enforcement interests;

(c) amend paragraphs 317JC(c), 317RA(g), 317ZAA(c) to specify that the 'legitimate interests of the DCP to whom the notice relates' include commercial interests;

(d) omit paragraphs 317JC(i), 317RA(g), 317ZAA(g) 'such other matters as the Director-General of Security or the chief officer, as the case requires, considers relevant';

(e) insert 'or' or 'and' after each matter listed;

(f) refer explicitly to the fundamental human right to privacy; or alternatively, refer to the Australian Privacy Principles under the Privacy Act and the potential privacy impact of a TAN or TCN be evidenced by a privacy impact assessment undertaken by the OAIC;

[88] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 7 [7].
[89] *Criminal Code Act 1995* (Cth) s 105A.12(4)(b).

(g) refer explicitly to a requirement of proportionality;

(h) include factors which require the issuer of a TAR, TAN or TCN to separately consider the potential legal consequences to the recipients of warrants; and

(i) require the decision maker to determine whether use of the measure is necessary in the investigation or enforcement of laws in relation to investigation or enforcement of a serious offence in circumstances where imperatives of law enforcement demonstrably outweigh reasonable expectations of confidentiality in communications of affected individuals and businesses.[90]

Conferral of criminal liability under the Criminal Code

102. As noted above, the Law Council considers there are many outstanding issues relating to the conferral of civil and criminal liability, which were not addressed by the Government amendments and which ought to be resolved.

103. The Law Council notes the general limitations placed on TARs, TANs and TCNs under sections 317ZG and 317ZH of the Act. As noted above, the Law Council supports the broadening of subsection 317ZG(1) to prohibit TARs from requiring a DCP to introduce a 'systemic weakness' or 'systemic vulnerability into a form of electronic protection. The Law Council also welcomes the amendment to subsection 317ZH(1) to allow for the general limits on TANs and TCN to apply also to TARs. This amendment is consistent with the recommendation from the Committee's report on the Bill.[91]

104. A TAR, TAN or TCN has no effect to the extent (if any) to which it would require a provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection,[92] or prevents a provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.[93] A TAR, TAN or TCN also does not have any effect to the extent (if any) to which it would require a provider to do an act or thing for which a warrant or authorisation is required.[94]

105. Paragraph 476.2(4)(b) of the Criminal Code was amended by the Act to allow that a person who causes any access to or modification of data held in a computer, or impairment of electronic communication to or from a computer, or any impairment to the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means, is entitled to do so under a TAR, TAN or TCN.[95]

106. Subsection 476.2(4) does not explicitly provide that a TAR, TAN or TCN which has no legal effect under sections 317ZG and 317ZH will not be conferred criminal immunity. There may be a legal argument that a TAR, TAN or TCN with no legal effect under sections 317ZG and 317ZH does not constitute a 'notice' under paragraph

[90] 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, 21-2 [41]-[45], 28-9 [75]-[76].
[91] 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, xiv [2.18].
[92] *Assistance and Access Act* s 317ZG(1)(a).
[93] Ibid s 317ZG(1)(b).
[94] Ibid s 317ZH(1)-(3).
[95] *Criminal Code Act 1995* (Cth) s 476.2(4)(b)(iv)–(vi).

476.2(4)(b)(iv)-(vi) of the Criminal Code. This issue was raised by the Law Council in its previous submission in relation to TANs and TCNs.[96]

107. Section 317ZGA was inserted by the Government amendments to allow for additional limits on TCNs. Subsection 317ZGA(1) provides that a TCN has no effect to the extent to which it requires a provider to ensure a telecommunications service or telecommunications system has a capability to enable a communication passing over the system to be intercepted, a capability to transmit lawfully intercepted information to applicable delivery points, or a delivery capability.[97]

108. The Law Council welcomes the additional limits on TCNs which seek to ensure that TCNs 'cannot modify, or qualify in any way, legislated obligations on providers in relation to interception capabilities, delivery capabilities and data retention.'[98]

109. However, it appears that the Law Council's concern regarding subsection 476.2(4) of the Criminal Code and the conferral of criminal immunity under ineffective notices extends to TCNs rendered ineffective under section 317ZGA.

110. The Law Council recommends that subsection 476.2(4) of the Criminal Code be further amended to explicitly state that a TAR, TAN or TCN given no legal effect under sections 317ZG and 317ZH, and a TCN given no legal effect under section 317ZGA , will not be conferred criminal immunity.

Accountability and oversight

111. The Government amendments have, to an extent, improved the reporting, notification, record-keeping obligations relating to the issuance of TARs, TANs and TCNs.

Notification

112. The notification requirements relating to TARs, TANs and TCNs have been improved by the requirement that ASIO or the Ombudsman (dependant on the interception agency which issued the notice) is notified within seven days about the issuance,[99] variation[100] or revocation[101] of a TAR, TAN or TCN. These amendments to the Act are consistent with the Law Council's recommendations from its previous submission for detailed reporting to the Ombudsman, and the Committee's report on the Bill.[102]

113. The Government amendments introduced subsections 317MAA(3) and (4), which require the Director-General of Security, when giving a TAN to a DCP, to inform the DCP of its right to make a complaint about the notice to the IGIS.[103] If the chief officer of an interception agency gives a TAN to a DCP, they are under the same obligation to inform

---

[96] 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, 21-2 [41]-[45], 28-9 [75]-[76].
[97] *Assistance and Access Act* s 317ZGA.
[98] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 26-7 [66]-[67].
[99] *Assistance and Access Act* ss 317HAB, 317MAB, 317TAB.
[100] Ibid ss 317JA(15)–(19), 317Q(12)–(14), 317X(6)–(8).
[101] Ibid ss 317JB(6)–(10), 317R(5)–(7), 317Z(3)–(5).
[102] 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, x [2.6].
[103] *Assistance and Access Act* ss 317MAA(3).

the DCP of its right to make a complaint to the Ombudsman or an authority that is the State or Territory inspecting agency in relation to the interception agency.[104]

114. The Law Council considers the obligation to inform DCPs of their right to complain as a positive step. However, it does not seem clear why this obligation applies only to the issuance of a TAN, and not for all Schedule 1 industry assistance notices. The Law Council considers that the Act should be amended so that any agencies issuing a TAR, TAN or TCN is obliged to inform the DCP who is receiving the notice of its right to complain to the relevant overseeing or inspecting body.

Record-keeping

115. The record-keeping requirements relating to TARs, TANs and TCNs have been improved by the requirement there must be a written record of oral advice from the relevant interception agency given to a DCP regarding their obligations relating a TAR, TAN or TCN.[105] These amendments to the Act are consistent with the Law Council's recommendations from its previous submission for clear record-keeping obligations.

Inspection by and reporting to the Ombudsman

116. The Law Council welcomes the introduction by the Government amendments of the Ombudsman's right to inspect records under new section 317ZRB. The Ombudsman may make a written report to the Home Affairs Minister on its inspections undertaken, and if the Ombudsman does make a written report, the Home Affairs Minister must table this report in Parliament.[106]

117. The Law Council notes that this inspection function of the Ombudsman is not mandatory. The Supplementary Explanatory Memorandum states that this reporting function of the Ombudsman 'complements the express powers to inspect records on the exercise of Part 15 powers including in the existing inspection regimes of the TIA Act and SD Act.'

118. The Law Council supports the introduction of this inspection measure, but it recommends that the inspection function of the Ombudsman be made mandatory. Further, the Law Council recommends that the Ombudsman's terms of reference in relation to its inspection obligation under section 317ZRB expressly include the protection of privacy of individuals.

Inspection and reporting by Minister

119. The reporting obligations to the Minister have been improved through the Government amendments. Subsection 94(2BA) was introduced into section 94 of the ASIO Act by the Government amendments. This subsection requires the annual report, prepared by the Director-General of Security for the Minister,[107] include a statement of the total number of TARs, TANs and TCNs issued during that period.[108] Subsection 94(2BB) was also introduced, requiring the Director-General of Security to include TCNs in the annual report prepared for the Minister where the TCN was directed towards

[104] Ibid ss 317MAA(4).
[105] Ibid ss 317HAA(5)–(6), 317MAA(5)–(6), 317TAA(1)–(3).
[106] Ibid ss 317ZRB(4), (6).
[107] *Public Governance, Performance and Accountability Act 2013* (Cth) s 46.
[108] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 94(2BA)(a)–(c).

assisting ASIO, despite the fact that the Attorney-General, not the Director-General of Security, has authority to give TCNs.[109]

120. The Law Council supports the fact that reporting on the number of TARs, TANs and TCNs issued is to Parliament as a whole. Subsection 94(3) of the ASIO Act requires a copy of the annual report to be given to the Leader of the Opposition in the House of Representatives and subsection 94(5), requires that the annual report be laid before each House of the Parliament. This amendment may improve the parliamentary oversight of the number of TARs, TANs and TCNs issued.

121. The Government amendments also introduced paragraph 317ZS(1)(d), improving the level of detail which the Home Affairs Minister's is required to include in its annual report under section 317ZS. The addition of paragraph 317ZS(1)(d) requires the inclusion of information on the kinds of serious Australian offences for which Schedule 1 powers are used in relation to.[110] This annual report is laid before Parliament.[111] This is consistent with the Law Council' recommendation that annual reports include a breakdown of the types of offences for which notices were issued.[112]

122. These amendments to the Act appear to be consistent with the Law Council's recommendations from its previous submission for detailed reporting to the relevant Minister.

Approval of Schedule 1 industry assistance notices

Decisions under Schedule 1 to be made by a judicial officer

123. In the Law Council's previous submission, it recommended that the Bill be amended so that decisions made under Schedule 1 are made by a judicial officer and not the Attorney-General. In the alternative, it recommended that judicial review of Schedule 1 decisions under the ADJR Act should be available.[113] The Law Council considers that these measures are necessary to ensure that the decision-making involves someone outside the agency itself, so that a more objective, external perspective is brought into the decision-making.

124. The Government amendments are not consistent with this recommendation. While the Government amendments introduce ministerial approval for TCNs, AFP Commissioner approval for TANs (see discussion below), and subsection 317WA(1) was introduced for a former judge to take on a role in the decision-making process or a TCN,[114] there is no requirement that for a judicial officer to be the primary decision maker for any Schedule 1 industry assistance notices.

125. The proposed amendments would require that a TAN or TCN cannot be issued or varied without the approval of an 'eligible judge'.[115] The proposed amendments would

[109] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 13 [24].
[110] *Assistance and Access Act* ss 317ZS(1)(a)–(d).
[111] *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(3).
[112] 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, 10.
[113] Ibid 21-2 [41]-[45], 31-2 [86]-[91].
[114] *Assistance and Access Act* ss 317WA(4)–(5).
[115] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8627 proposed amendment (4), (6) (for TANs), (9), (11) (for TCNs); Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8627 proposed amendment (2). The proposed amendments provide that

require an eligible judge to refuse the issuance or variation of a TAN or TCN unless satisfied that:

(a) the DCP to whom the notice is to be given can comply with the notice;

(b) the notice can validly be given under this Part;

(c) a provision of this Part does not prevent the notice from having effect; and

(d) the DCP has, if reasonably practicable, been consulted and given a reasonable opportunity to make submissions on whether the requirements to be imposed by the notice are reasonable and proportionate and whether compliance with the notice is practicable and technically feasible.[116]

126. The Law Council supports this proposed amendment as it would introduce judicial oversight for the issuance of Schedule 1 industry assistance notices.

Ministerial approval for TCNs

127. The Government amendments added the requirement that the Attorney-General must obtain ministerial approval before the issuance of a TCN.[117] This provides layer of approval for TCNs that did not exist in the Bill.[118] The Law Council supports this amendment.

128. This amendment appears consistent with the recommendation in the Committee's report on the Bill that TCNs 'be jointly authorised by the Attorney-General and the Minister for Communications.'[119]

129. However, when the Minister is considering whether to approve the issuance of a TCN, the decision-making criteria to which the Minister must have regard is far less extensive than the decision-making criteria in relation to a TAR, TCN or TAN.[120] These factors include:

(a) the objectives of the notice;

(b) the legitimate interests of the DCP to whom the notice relates;

(c) the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry;

(d) the representation (if any) that was made under subsection (4); and

(e) such other matters (if any) as the Minister considers relevant.

130. The Law Council supports the inclusion of the 'legitimate interests' of the DCP. Under subsection 317TAAA(4), the Attorney-General may make a representation to the Minister about the proposal to give the TCN, which may deal with any of the matters set

---

an 'eligible judge' would be a judge who is declared by the Minister to be an 'eligible judge' for the purposes of the Act.

[116] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8627 proposed amendment (5), (7) (for TANs), (10), (12) (for TCNs).

[117] *Assistance and Access Act* s 317TAAA(1).

[118] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 s 317T(1).

[119] 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, xi [2.9].

[120] *Assistance and Access Act* s 317TAAA(6).

out in the 'reasonable and proportionate' criteria for decision-making in relation to a TCN. It is important to note that the Attorney-General is under no obligation to make a representation. Therefore, there is no guarantee under the Act that the Minister's decision to approve the issuance of a TCN to a DCP considers whether the issuance is reasonable and proportionate. Consequently, section 317TAAA introduces the potential risk that a TCN given to a DCP is not reasonable and proportionate.

131. As the Minister has the final say on whether a TCN will be given to a DCP, the Law Council recommends that section 317TAAA be amended so that the Minister is required to apply the decision-making criteria as contained in sections 317JAA, 317P and 317V, and consequently, be required to consider the same matters listed in sections 317JC, 317RA, 317ZAA, to ensure the issuance of the TCN is reasonable and proportionate.

Ministerial approval under Intelligence Services Act 2001 (Cth)

132. As mentioned above, under subsection 317ZH(1), a TAR, TAN or TCN does not have any effect to the extent (if any) to which it would require a provider to do an act or thing for which a warrant or authorisation is required particular laws.[121] Those particular laws are listed in paragraphs 317ZH(1)(a)–(g). The Government amendments appear to add clarity to section 317ZH regarding the prohibition against the side-stepping of warrants:

(a) 'that relates to an agency' has been inserted into subsection 317ZH(1), seeking to clarify that the prohibition in subsection 317ZH(1) extends to warrants and authorisations that the particular agency would require; and

(b) 'the agency, or an officer of the agency, would be required to have or obtain' has been inserted into subsection 317ZH(1), seeking to clarify that TAR, TAN or TCN is not intended to require a provider to do an act or thing that, if done by an agency or an officer of an agency, which would require a warrant or authorisation under a law provided in paragraphs 317ZH(a)–(g).[122]

133. The introduction of paragraph 317E(1)(da) appears to further bolster the safeguard against TARs, TANs or TCNs including requirements which would otherwise require a warrant or authorisation. Paragraph 317E(1)(da) provides a 'listed act or thing' for the purposes of industry assistance provisions is one done to assist in or facilitate giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory, or the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory. Paragraph 317E(1)(da) underscores that a TAR, TAN or TCN can only be issued to require one of the listed things be done by a provider where a valid warrant is in force to authorise the activity.

134. The Law Council supports these additions which seek to sure that TARs, TANs and TCNs are not being used as a substitute for warrants or authorisations.

135. The Law Council noted that the Government amendments omitted paragraph 317ZH(1)(e), which removed the IS Act. The IS Act requires the Australian Secret Intelligence Service and the Australian Signals Directorate to gain ministerial approval before, for example, undertaking activities for the purposes of producing intelligence on an Australian person.[123]

---

[121] Ibid s 317ZH(1)-(3).
[122] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 46 [3].
[123] *Intelligence Services Act 2001* (Cth) s 8(1)(a)(i).

136. By omitting paragraph 317ZH(1)(e), a TAR, TAN or TCN would not be rendered to have no effect if it required a DCP to do any act or thing which would otherwise require ministerial approval under the IS Act.

137. The Supplementary Explanatory Memorandum states:

> *The amendment is intended to resolve the ambiguities that arise from explicitly including the Intelligence Services Act 2001 (Cth) and the ministerial authorisations within that Act that do not apply to the agencies limited by 317ZH*.[124]

138. The Supplementary Explanatory Memorandum states the reason for the removal is so that agencies under 317ZH are limited by the warrants or authorisations that they themselves would require, rather than a warrant or authorisation that another authority would require to lawfully do the things within the notice.[125]

139. The Law Council is concerned that this Government amendment may allow for the situation where intelligence agencies could approach issuing agencies, and vice-versa, with the intention of side-stepping a process that would otherwise require a warrant or authorisation under the IS Act. The Committee should be satisfied that the removal of the IS Act from subsection 317ZH(1) would not allow for this to occur.

AFP Commissioner approval for TANs issued by chief officer of interception agency of State or Territory

140. The Government amendments inserted section 317LA, which requires that, prior to the issuance of a TAN to a DCP, the chief officer of an interception agency of a State or Territory must provide the AFP Commissioner with a written notice setting out a proposal to give the TAN, and that AFP Commissioner must approve the giving of the TAN.

141. This amendment appears consistent with the recommendation in the Committee's report on the Bill that TANs 'be submitted for approval to the Commissioner of the AFP before being issued to the recipient... to ensure consistency in decision making, and reporting, across jurisdictions.'[126]

142. The AFP Commissioner is not required to apply the same statutory criteria as if it were the original issuing body.[127] In fact, it is not required to apply any statutory criteria.

143. The Supplementary Explanatory Memorandum suggests that, in the approval process of TANs, the AFP will not act as a secondary and final decision-maker, but instead will provide a 'rubber stamp' to the decisions made by the chief officer of an interception agency of a State and Territory:

> *The AFP will not overrule legitimate operational decisions by State and Territory agencies as part of this approval process*.[128]

144. The role of the AFP Commissioner under section 317LA is not consistent with the Committee's recommendation that the AFP Commissioner must apply the same

---

[124] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 47 [10].
[125] Ibid 47 [10].
[126] 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, ix [2.8].
[127] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* s 317P.
[128] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 25 [124].

statutory criteria, and go through the same decision-making process, as would apply if the AFP were the original issuing authority.[129]

145. The Law Council supports the proposed amendment which would require the that AFP Commissioner not give approval for the issuance of a TAN unless satisfied of the matters specified in section 317P.[130]

146. Notwithstanding this, it seems that the intended role of the AFP Commissioner is one of centralisation and co-ordination:

> *The section reflects the coordination role of the AFP Commissioner. Centralisation will reduce duplicate requests, enable the exchange of relevant information across jurisdictions (for example, where a provider has previously been unable to assist law enforcement) and advise on the types and forms of assistance commonly requested. The AFP will also maintain preferred points of contact within agencies and providers, establish processes with providers and agencies for the efficient and effective delivery of notices and ensure consistency in payment and cost recovery. It may also serve as a central point for statistics about how the powers are being used.*[131]

147. Therefore, and in the alternative to subjecting the AFP Commissioner to decision-making criteria, if it is intended that the AFP Commissioner have a consultative and coordination role in the issuance of TANs by a state or territory interception agency, the Law Council recommends that section 317LA be amended to expressly state this role of the AFP Commissioner.

Costs

148. The Government amendments insert paragraphs (c) to (f) in subsection 317ZK(3). This amendment provides that the DCP must comply a requirement under a TAN or a TCN on the basis that the provider neither profits from complying nor bears the reasonable costs of complying, unless:

(a) the provider and the applicable costs negotiator otherwise agree; or

(b) in the case of a requirement under a TAN given by the Director-General of Security, or the chief officer of an interception agency - the Director-General of Security or the chief officer declares in writing that it is satisfied that it would be contrary to the public interest for this subsection to apply to the requirement; or

(c) in the case of a requirement under a TCN - the Attorney-General declares in writing that the Attorney-General is satisfied that it would be contrary to the public interest for this subsection to apply to the requirement.

149. New subsection 317ZK(3A) sets out the matters which must be considered by the Director-General of Security, the chief officer or the Attorney-General in deciding whether the subsection 317ZK(3) presumption (as to who should bear the cost of assistance) should apply:

---

[129] 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, ix-x [2.5].
[130] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8625 proposed amendment (2).
[131] Supplementary Explanatory Memorandum, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 25 [124].

(a) the interests of law enforcement (in the case of an interception agency);

(b) the interests of national security (in the case of ASIO);

(c) the objects of this Act;

(d) the extent to which compliance with the requirement will impose a regulatory burden on the provider;

(e) the reasons for the giving of the technical assistance notice or technical capability notice, as the case requires; and

(f) such other matters (if any) as the Director-General of Security, the chief officer or the Attorney-General, as the case may be, considers relevant.

150. The Supplementary Explanatory Memorandum states:

> *the measures in 317ZK set a high threshold for exercising the public interest exemption in subsection 317ZK(3) by requiring that the decision-maker take into account a range of commercial, law-enforcement and security considerations*.[132]

151. The Law Council disagrees that the measures in section 317K set a high threshold. In the view of the Law Council, subsection 317K(3A) broadly captures the matters which are considered to be relevant. Further, there is the potential risk that it could be determined that the interests of law enforcement and national security outweigh the regulatory burden on the provider because it is in the interests of the former that its resources and funding be directed at its other efforts in law enforcement and national security.

152. Consistent with the Law Council's previous recommendation that additional resources for oversight of the activities under Schedule 1 should be made available to the relevant oversight bodies, it recommends that the Government should provide adequate funding for its amendments. In this instance, the relevant issuing agencies should receive adequate funding to bear the costs of a DCP's compliance with a Schedule 1 notice.

Schedule 2 – Computer Access Warrants

Compensation

153. The Law Council recommended in its previous submission that section 64 of the SDA be amended to ensure liability by the Commonwealth to pay compensation for loss or injury resulting from the unlawful use of a computer access warrant.

154. The Government amendments introduced subsection 64(2) to provide for the circumstances in which the Commonwealth is liable to pay a person who has suffered loss or injury flowing from a computer access warrant.

155. The Commonwealth is liable to pay compensation to a person when that person has suffered loss or injury:

[132] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 25 [124].

a) from the use of a computer, a telecommunications facility operated or provided by the Commonwealth or a carrier, any other electronic equipment or a data storage device, for the purpose of obtaining access to data held therein;

b) where the use of the computer, facility, equipment or device as by the AFP, the Integrity Commissioner or staff member of the ACLEI; and

c) the use is:

a. prohibited by law of the State or Territory in which the use occurs; and

b. neither in accordance with the SDA or in performance of a function, or the exercise of a power, conferred by Commonwealth law.[133]

156. The amount to paid to the person is the amount of compensation that is agreed between the person and the Commonwealth or, in default of such an agreement, the amount of compensation that is determined in a court.[134]

157. It appears that s 64(2) of the SDA is consistent with the Law Council's recommendation.

Emergency authorisations

158. Emergency authorisations for access to data held in a computer are created under subsection 32(2A) of the SDA and would allow 'anything that a computer access warrant may authorise'. Under new paragraph 27E(2)(h) of the SDA, a computer access warrant would allow agencies to intercept communications over a telecommunications system.

159. This was inconsistent with the former subsection 32(4) of the SDA which stated that '[n]othing in this Part authorises the doing of anything for which a warrant would be required under the [TIA Act]'.

160. In the Law Council's previous submission, it recommended that section 32 of the SDA be amended to outline that telecommunications intercepts will not be permitted under emergency authorisations as consistent with the former subsection 32(4) of the SDA.[135]

161. However, the phrase '(other than subsection (2A) of this section)' was inserted into section 32(4) of the SDA by the Government amendments. The effect of this amendment is that telecommunications intercepts are expressly permitted under emergency authorisations.

162. In its previous submission, the Law Council noted that attaching telecommunications interception power to computer access warrants involves a reduction in the threshold for telecommunications interception.[136] Previously, under the TIA Act where a law enforcement agency applies 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

[133] *Surveillance Devices Act 2004* (Cth) ss 64(2)(a)–(d).
[134] Ibid ss 64(e)–(f).
[135] 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].
[136] Ibid.

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.[137] As noted above, serious offences are 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.

163. The 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 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.

164. The Law Council is concerned that the amendment to subsection 32(4) of the SDA permits telecommunication interceptions under computer access warrants which have received emergency authorisation, meaning they have not been approved by an eligible Judge or a nominated AAT member, and these warrants can be issued for a much broader range of offences.

165. The Law Council recommends that section 32 of the SDA be amended to outline that telecommunications intercepts will not be permitted under emergency authorisations as consistent with the former subsection 32(4) of the SDA.[138]

Removal of computer or other things from premises

Scope

166. The Law Council reiterates its concerns regarding the temporary removal of computers and other things under s 25A of the ASIO Act and s 27E of the SDA.[139] The temporary removal power is too broad as it allows the Attorney-General or Judge or nominated AAT member to authorise the temporary removal of computers or other things from premises for the purpose of entering specified premises or gaining entry to or exiting specified premises.[140] It is unclear why this power is necessary or justified.

167. In the absence of such justification, the temporary removal power should be limited to the purpose of obtaining access to 'relevant data' under existing paragraphs 25A(4)(a), (ab) and 27E(2)(c) and (d) of the ASIO Act and 27E(2)(c) of the SDA.

168. The temporary removal power is also too broad as it allows the temporary removal of 'other things' with the potential to apply to any object on the premises in an arbitrary manner.

---

[137] *Telecommunications Act (Assistance and Access) Act 1979* (Cth) s 46(1)(d).
[138] 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].
[139] 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, 41-2 [122]-[127].
[140] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4)(a)-(ab), 27E(2)(c)-(d); *Surveillance Devices Act 2004* (Cth) s 27E(2)(d).

169. The criteria for what objects may be temporarily removed should be clearly set out in the legislation to ensure that there is a rational connection with the legitimate objective of the legislation.

170. The Law Council was concerned that there was no maximum time limit for the temporary removal of computers and other things in the Bill, with the potential for there to be an indefinite retention of such items. The Law Council considered that this was not is proportionate, particularly given the importance of computers in a person's daily life.

171. The Government amendments introduce subsections 25A(4A), 27E(3A) and 27E(2A) into the ASIO Act. These subsections require that if a computer or thing is removed from premises in accordance with a warrant[141] or authorisation,[142] the computer or thing must be returned to the premises when returning the computer or thing would no longer be prejudicial to security (if returning the computer or thing would be prejudicial to security), or otherwise within a reasonable period.

172. It appears that the maximum time limit for the temporary removal of computers and other things is 'when returning the computer or thing would no longer be prejudicial to security' or within 'a reasonable period'. The Law Council considers that these time-limits are ambiguous and would be open to interpretation.

173. The Law Council recommends that subsections 25A(4A), 27E(3A) and 27E(2A) of the ASIO Act be amended to introduce a concrete, quantifiable time-limit for the return of computers, and a requirement that the removal of a computer for any time after the prescribed time-limit must be an approved extension from a court.

Concealment of access

174. Subsections 25A(8), 27A(3C) and 27E(6) of the ASIO Act and paragraphs 27E(7) of the SDA would authorise specified concealment activities while the warrant is in force, up to 28 days after the warrant ceases to be in force, or as soon as reasonably practicable after the 28-day period. These concealment activities could include for example anything reasonably necessary to conceal the fact that anything has been done under the warrant or:

(a) entry to premises, including third-party premises;

(b) removal and return of computers or other things from premises;

(c) the use of other computers or communications in transit, including, if necessary, adding, copying, deleting or altering data in the computer or the communication in transit;

(d) the interception of telecommunications; and

(e) other things reasonably incidental to these activities.

Automatic concealment authorisation and duration

175. The Law Council maintains its concerns raised in its previous submission regarding the automatic authorisation of concealment activities under subsections 25A(8),

[141] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4A), 27E(2A).
[142] Ibid s 27E(3A).

27A(3C) and 27E(6) of the ASIO Act and paragraphs 27E(7) of the SDA, and the absence of a time-limit by which concealment of access powers may be exercised.[143] Neither of these issues have been resolved by the Government amendments.

176. Concealment activities can be done 'at any time while the warrant is in force or within 28 days after it ceases to be in force'.[144] However, if nothing has been done within the 28 day period to conceal the fact a computer has been accessed, they may be authorised 'at the earliest time after the 28-day period at which it is reasonably practicable' to conceal access to a computer under warrant.[145]

177. The Law Council expressed concerned that the absence of a time-limit by which concealment of access powers may be exercised may authorise privacy-intrusive activities in the absence of the reasonable grounds threshold which underpin the initial warrant. It recommended that paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) of the ASIO Act and paragraphs 27E(7)(k) of the SDA should not proceed. In the alternative, it recommended that ASIO should be able to apply to the Attorney-General (or in the case of an identified person warrant the Director-General) for an extension of time with a maximum limit where it is necessary for the concealment of access.

178. The Government amendments did not omit paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) of the ASIO Act and paragraphs 27E(7)(k) of the SDA, nor require ASIO to be request an extension of time from the Attorney-General. Rather, the Government amendments inserted section 49B in the SDA, which requires that the Ombudsman is notified when an act or thing is done to conceal access under a computer access warrant more than 28 days after the warrant has expired. The chief officer of the law enforcement agency must notify the Ombudsman within seven days after the things was done.

179. In the view of the Law Council, a requirement to notify the Ombudsman is not a sufficient safeguard to ensure that a chief officer of a law enforcement agency cannot exercise powers that may authorise privacy-intrusive activities in the absence of the reasonable grounds threshold which underpin the initial warrant.

180. The Law Council maintains its view that the Act should not allow an act or thing be done to conceal access under a computer access warrant more than 28 days after the warrant has expired. It recommends that the ASIO Act and the SDA be amended to omit paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) from the ASIO Act and paragraph 27E(7)(k) from the SDA.

Safeguards

181. The Law Council previously expressed concerns about the concealment provisions in the ASIO Act and the SDA not including the safeguards regarding 'certain acts not authorised' which applied to the computer access warrants under the ASIO Act.[146] That is, they did not appear to include the limitations on any damage or loss caused by the concealment activities. The Law Council recommended that these safeguards should

[143] 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, 43-4 [131]-[133], [135]-[137].
[144] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(8)(j), 27E(6)(j); *Surveillance Devices Act 2004* (Cth) s 27E(7)(j).
[145] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(8)(k), 27E(6)(k); *Surveillance Devices Act 2004* (Cth) s 27E(7)(k).
[146] 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, 43 [134].

be present for the new concealment powers to assist in the proportionality of the measures.

182. The Government amendments introduced subsections 25A(9) and 27A(3D) into the ASIO Act and subsection 27E(8) into the SDA. These sections provide that the concealment of access provisions do not authorise the doing of anything that is likely to:

(a) materially interfere with, interrupt or obstruct a communication in transit, or the lawful use by other persons of a computer, unless the thing is necessary to do one or more of the things specified in the concealment of access provisions; or

(b) cause any other material loss or damage to other persons lawfully using a computer.

183. It appears that this amendment is consistent with other provisions in the ASIO Act which refer to 'material loss or damage'. However, these provisions require the loss or damage caused to be 'material' loss or damage in order for the act or thing to be deemed 'unauthorised' under paragraphs 25A(9)(b) and 27A(3D)(b) of the ASIO Act and paragraph 27E(8)(b) of the SDA. The requirement that the loss or damage be 'material' sets a higher bar than 'cause *any* loss or damage' – a bar which may be too high for a person to be able to access compensation for loss or damage.

184. The Law Council recommends that these sections be amended to omit the requirement of 'material'.

185. The Government amendments also introduced subsections 25A(10) and 27A(3E) into the ASIO Act and subsection 27E(9) into the SDA, which require that if a computer has been removed from a place in accordance with the concealment of access provisions,[147] the computer must be returned within a reasonable period. The Law Council welcomes the time-limit on the removal of computers under the concealment of access provisions, but still considers that there should be a quantifiable maximum time-limit by which a computer must be returned. The current requirement of 'a reasonable period' is ambiguous.

186. The Law Council recommends that subsections 25A(10) and 27A(3E) in the ASIO Act and subsection 27E(9) in the SDA be amended to include a quantifiable time-limit by which a computer which has been removed in accordance with the concealment of access provisions must be returned.

Authorised disclosures

187. The Government amendments improve the authorised disclosures relating to general computer access intercept information. The Law Council supports the introduction of these measures as they permit authorised disclosures to the investigative bodies of the Ombudsman and IGIS.[148]

188. The Government amendments introduced subsections 63AB(3)–(6) and 63AC(3)–(6) into the TIA Act. These subsections relate to restrictions on the use and disclosure restrictions on 'general computer access intercept information' and 'ASIO general

[147] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(8)(f), 27E(6)(f); *Surveillance Devices Act 2004* (Cth) s 27E(7)(f).
[148] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 23AB(3)–(5), 63AC(3)–(5).

computer access intercept information'. They permit disclosure to the Ombudsman, or the IGIS for ASIO general computer access intercept information.

189. New subsection 63AB(3) states that a person may, in connection with the performance by an Ombudsman official of the its functions or duties or the exercise by an Ombudsman official of the Ombudsman official's powers communicate to the Ombudsman official, make use of, or make a record of, 'general computer access intercept information'. The same is permitted for an IGIS official in relation to 'ASIO general computer access intercept information' under subsection 63AC(3). An Ombudsman official, or an IGIS official, is permitted to communicate this information to another person, or make use of or record the information under subsections 63AB(4) and 63AC(4). The meaning of 'general computer access intercept information' is information obtained under a general computer access warrant by intercepting a communication passing over a telecommunications system. Subsections 63AB(6) and 63AC(6) permit disclosure to the Ombudsman, or to the IGIS, in instances where information was obtained by intercepting a communication passing over a telecommunications system and the interception was purportedly for the purposes of doing a thing specified in a general or ASIO computer access warrant, and the interception was not authorised by the general or ASIO computer access warrant.

190. Paragraph 317ZF(3)(b) allows a person to make an authorised disclosure of TAR, TAN or TCN information for the purposes of any legal proceeding, and subsection 317ZF(3) allows such information to be disclosed for the purposes obtaining legal advice, in relation to Part 15 of the Telecommunications Act.

191. In the ASIO Act, section 34ZS provides secrecy provisions relating to warrants and questioning. Paragraph 34ZS(5)(c) provides that a 'permitted disclosure' means a disclosure to a lawyer for the purpose of obtaining legal advice with a warrant issued under Division 3 of the ASIO Act, or obtaining representation in legal proceedings seeking a remedy relating to such a warrant or the treatment of a person in connection with such a warrant. However, this 'permitted disclosure' only applies to legal advice relating to questioning and detention warrants, and not to computer access warrants under section 24A of the ASIO Act.

192. Division 1 of Part 6 of the SDA relates to restrictions on use, communication and publication of information. Subsection 44(b) makes any information relating to the application for, the issue of, the existence of or the expiration of, a warrant or an emergency authorisation, 'protected information'. Subsections 45(1) and 45(2) make it an offence to use, record, communicate or public any protected information, carrying a sentence of 2 years imprisonment, or 10 years imprisonment if the disclosure prejudices the effective conduct of an investigation. Subsection 45(3) provides that protected information may not be admitted in evidence in any proceedings. Paragraph 45(2)(a) provides that subsections 45(1)–(3) do not apply to information that has been disclosed in proceeding in open court lawfully. Therefore, the SDA does not permit disclosures for the purpose of obtaining legal advice in relation to computer access warrants under Division 4 of Part 2 of the SDA.

193. The Law Council recommends that the ASIO Act and the SDA be amended to permit disclosures about computer access warrants under Division 4 Part 2 of the SDA and under section 25A of the ASIO Act for the purpose of obtaining legal advice.

Schedule 5 – Voluntary assistance to ASIO

Procedural matters

194. Subsection 21A(1) of the ASIO Act confers an immunity from civil liability on persons or bodies who render voluntary assistance to ASIO in accordance with a request by the Director-General of Security, or a senior position-holder to whom the Director-General has delegated the power under subsection 16(1A). This proposed internal authorisation would represent a significant expansion of power, as previously only the Attorney-General could confer a civil or criminal immunity on participants in a special intelligence operation.

195. As expressed in the Law Council's previous submission, it considers that the procedural framework surrounding requests made under subsection 21A(1) and the associated immunity from civil liability should be improved in the following ways to aid transparency and accountability by making it clear:

a) that compliance with a request is voluntary (as proposed for subsection 317HAA(1) of the Telecommunications Act);

b) how long the request will be in force with a maximum statutory period applying;

c) that a voluntary assistance provided to ASIO request does not cover ongoing requirements for assistance;

d) that oral requests should be followed by a written record to the person as soon as reasonably practicable;

e) the manner in which such requests may be varied or revoked; and the manner in which there are reporting requirements under the provisions. The Law Council considers that there should be annual reporting to the Parliament on the number of times the provision is used; the kinds of assistance requested and provided; and the extent to which the civil immunity provision did not apply.

196. The Government amendments introduced subsections 21A(2), (2A) and (3A) into section 21A of the ASIO Act. Subsections 21A(2) and (2A) require that an oral request for voluntary assistance under paragraph 21A(1)(a) must be in writing unless the making of the request should be made as a matter of urgency, would be prejudicial to security, or would be prejudicial to the operational security of the organisation.[149] It appears that the effect of subsections 21A(2) and 21A(2A) is that the circumstances in which a request may be made orally has been confined. The Law Council considers that the confining of oral requests in these circumstances only as an improvement as it appears to assist in clarity of responsibilities for ASIO.

197. In relation to point (d) above, the notification requirements have been improved by the introduction of subsection 21A(3A) into section 21A of the ASIO Act. The Bill already required that oral requests be followed by a written record by the Director-General.[150] But the introduction of subsection 21A(3A) places an additional obligation on the Director-General to notify the IGIS that a request has been made, within seven days after the request was made.

[149] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 21A(2)(a)–(c).
[150] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill (2018) s 21A(3).

198. In relation to point (f) above, subsection 94(2BC) was introduced into section 94 of the ASIO Act by the Government amendments. This subsection requires the annual report, prepared by the Director-General of Security for the Minister,[151] include a statement of the total number of requests made under paragraph 21A(1)(a) during the period,[152] as well as the total number of orders made under subsection 34AAA(2) during the period.[153]

199. The Law Council supports the fact that reporting on the number of requests for voluntary assistance by ASIO, and the number of orders requiring assistance, is to Parliament as a whole. This amendment may improve the parliamentary oversight of the number of TARs, TANs and TCNs issued.

200. However, this amendment is only partly consistent with the Law Council's recommendation, as the Director-General is not required to include in the annual report the kinds of assistance requested and provided and the extent to which the civil immunity provision did not apply. As already mentioned, the Government amendments introduced paragraph 317ZS(1)(d), which requires the Home Affairs Minister's to include in its annual report information on the kinds of serious Australian offences in which TARs, TANs and TCNs are issued, which is then laid before Parliament.[154]

201. The Law Council considers that including in the annual report the kinds of circumstances in which voluntary assistance (under paragraph 21A(1)(a)), and compulsory orders (under subsection 34AAA(2)), are being requested may assist the Parliament in ensuring that the powers are being used proportionately.

Schedule 5 - Compulsory assistance to ASIO

Procedural matters

202. As noted above, there are many outstanding issues relating to section 34AAA, which relate to issues such as the detention for non-compliance with the order, the lack of requirements to guard against oppressive use of multiple coercive powers to obtain particular information and the lack of adequate record keeping requirements, reporting requirements, instructions for the cessation of activities and destruction of materials, at least consistent with other parts of the ASIO Act.

203. In the Law Council's previous submission, it recommended that section 34AAA should include adequate record keeping requirements, reporting requirements instructions for the cessation of activities and destruction of materials at least consistent with other parts of the ASIO Act.

204. The Government amendments appear to have addressed some procedural issues with requests from ASIO for compulsory assistance relating to data. The record-keeping requirements have been improved by the introduction of subsections 34AAA(3A) and (3B), requiring the Director-General to make a written record of a verbal request within 48 hours.[155] New paragraph 34AAA(3C) requires that a request for compulsory assistance must be accompanied by a statement setting out the particulars and outcomes of all previous requests (if any) for the making of an order relating to the person specified in the current request.

---

[151] *Public Governance, Performance and Accountability Act 2013* (Cth) s 46.
[152] *Australian Security Intelligence Organisation Act 1979* (Cth) s 94(2BC)(a).
[153] Ibid s 94(2BC)(b).
[154] *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(3).
[155] *Australian Security Intelligence Organisation Act 1979* (Cth) s 34AAA(3A)–(3B).

205. Instructions for the cessation of activities have been introduced by the Government amendments. Paragraphs 34AAA(3D) and (3E) require that, if the grounds on which an order under section 34AAA was made have ceased to exist, the Director-General must inform the Attorney-General and, if the Attorney-General is also satisfied that the grounds have ceased to exist, the Attorney-General must revoke the order.

206. The record-keeping requirements have been improved by the introduction of subsection 34(1A), which provides that if an order was made under subsection 34AAA(2) in relation to the warrant (regarding a person with knowledge of a computer or a computer system to assist access to data), then the report must also include details of the extent to which compliance with the order has assisted the ASIO in carrying out its functions. Subsection 34ZH(2) requires that if an order was made under subsection 34AAA(2) in relation to accessing data that was held in, or accessible from, a computer or storage device that was seized under section 34ZB, the report must also include details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions.

207. The outstanding issues regarding reporting of requests made under subsection 34AAA(1) are detailed above.

Parliamentary Privilege

208. The Government amendments attempt to provide clarity regarding the relationship of Act to parliamentary privileges and immunities. Section 317RZ of the Act, section 27J of the SDA, section 3SA of the Crimes Act and section 202B of the Customs Act provide (respectively) that Part 15 of the Act, Division 4 (Computer access warrants) of Part 2 of the SA, Division 2 of Part IAA of the Crimes Act, Subdivision C of Division 1 of Part XII of the Customs Act do not affect the law relating to the powers, privileges and immunities of either House of the Parliament or the members, committees or joint committees of either House of Parliament.

209. This recommendation is consistent with the Committee's recommendation in its report on the Bill that it include an amendment which puts beyond any doubt that the Bill may impact parliamentary privilege.[156]

210. The Law Council supports these amendments as they are broad provisions which maintain that parliamentary privilege is not abrogated, rather than limited approach that only permits limited disclosures.

[156] 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 [2.16].

Law Council
OF AUSTRALIA

Office of the President

20 February 2019

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6201
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Chair

***Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)**

1. Thank you for the opportunity for the Law Council to provide an additional written submission to the Parliamentary Joint Committee on Intelligence and Security's (**the Committee**) inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**the Assistance and Access Act**).

2. This submission provides comment on the amendments sought to be introduced by the Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 (**the Miscellaneous Amendments Bill**), as well as the amendments to the Miscellaneous Amendments Bill introduced by the Opposition.

3. The Law Council notes that while the amendments proposed by the Miscellaneous Amendments Bill would be an improvement to the changes to the Telecommunications Act as introduced by the Assistance and Access Act, the amendments do not address all of the matters raised in the Law Council's submission to the Committee dated 23 January 2019 (**preliminary submission**).

4. In particular, the amendments to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (**the Assistance and Access Bill**) introduced in the Senate in December 2018, but never passed, included an amendment to introduce judicial oversight of the issuance of notices under Part 15 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**).[1] However, this amendment has not been included in the amendments to the Miscellaneous Amendments Bill. The Law Council reiterates that the Act should require judicial oversight for the issuance of Schedule 1 industry assistance notices.

[1] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) sch 1 items (1)-(12).

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

The Bill

5. The Miscellaneous Amendments Bill proposes to amend paragraph 6(1D)(b) of the *Independent National Security Legislation Monitor Act 2010* (Cth) to require the Independent National Security Legislation Monitor (**INSLM**) to review the Assistance and Access Act before the end of the 18-month period beginning on the date the Assistance and Access Act received Royal Assent on 8 December 2018.[2] The Law Council considers that this amendment was required due to the hasty manner in which the Assistance and Access Act was passed in December 2018. Nonetheless, as expressed in the Law Council's preliminary submission, the Law Council supports the review of the Assistance and Access Act by the expert body.[3]

6. Schedule 2 of the Miscellaneous Amendments Bill proposes to reintroduce the Australian Commission for Law Enforcement Integrity and state and territory independent commissions against corruption to the list of agencies deemed to be an 'interception agency' for the purposes of Part 15 of Telecommunications Act. The Law Council recognises that the exclusion of these agencies from the list of 'interception agency' in the Assistance and Access Act, as passed by both houses in December 2018, was consistent with the Committee's recommendation in its Advisory Report on the Assistance and Access Bill.[4] The Law Council acknowledges the Committee's statement that the Miscellaneous Amendments Bill proposes to reinclude the above-mentioned agencies in the list of 'interception agency' on its recommendation.[5] The Law Council does not oppose this amendment.

The Opposition's amendments to the Miscellaneous Amendments Bill

7. On 14 February 2019, amendments introduced by the Opposition to section 317ZG of the Telecommunications Act, and the related definitions in 317B, were passed by the Senate.[6] The Law Council supports these amendments to 'systemic weakness or systemic vulnerability' in the Telecommunications Act, as was noted in the Law Council's preliminary submission.[7]

8. Further amendments to the Miscellaneous Amendments Bill, yet to be voted on in the Senate, include amendments to limit technical assistance requests (**TAR**) and technical assistance notices (**TAN**) to 'listed acts or things'.[8] In the Law Council's preliminary submission, the Law Council supported the Government amendments to the Assistance and Access Bill which sought to render the 'listed acts or things' exhaustive.[9]

---

[2] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 sch 1 item 1.
[3] Law Council of Australia, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (23 January 2019) 27.
[4] 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, ix [2.4].
[5] Commonwealth, *Parliamentary Debates,* House of Representatives, 12 February 2019, 76 (Tony Smith).
[6] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 sch 3 items 1-6.
[7] Law Council of Australia, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (23 January 2019) 27-31.
[8] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 sch 4 items 1-4.
[9] Law Council of Australia, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (23 January 2019) 24.

The proposed amendments to the Miscellaneous Amendments Bill appear to have the same intended effect and are therefore supported by the Law Council.

9. The Law Council supports the proposed amendment to the Miscellaneous Amendments Bill to require the Australian Federal Police Commissioner (**AFP Commissioner**) to apply to the same statutory criteria, and to undertake the same decision-making process, as would apply if the AFP Commissioner were the original issuing authority of the TAN.[10]

10. The Law Council supports the proposed amendment to the Miscellaneous Amendments Bill which would not allow the Home Affairs Minister to delete certain information from a report prepared by the Commonwealth Ombudsman before tabling the report in Parliament.[11] The Law Council considers that this amendment strengthens the oversight and accountability measures for the operation of Part 15 of the Telecommunications Act.

[redacted]

Yours sincerely

[redacted]

Arthur Moses SC
President

[10] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 sch 5. See Law Council of Australia, Submission No 4 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (23 January 2019) 44-5.
[11] Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 sch 7.