Law Council
OF AUSTRALIA

Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Independent National Security Legislation Monitor

11 November 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 14 September 2019 are:

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

Executive Summary

1. The Law Council welcomes the opportunity to provide a submission to the Independent National Security Legislation Monitor's (**INSLM**) review into the operation, implications and effectiveness of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**). This statutory review is being conducted by the INSLM following a referral by the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) made under section 7A of the *Independent National Security Legislation Monitor Act 2010* (Cth).[1]

2. The Law Council notes that the Committee is conducting a concurrent review of the TOLA Act, with the INSLM's review set to inform that process. The Committee's review is due to be completed by 30 September 2020.

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

4. The primary concern of the Law Council is ensuring the policy objective of the TOLA Act, to increase public safety by providing faster access to encrypted data, are appropriately balanced and that the measures provided in the TOLA Act are reasonable, necessary and proportionate, including by incorporating transparent and verifiably reliable safeguards and controls.

5. To this end, the Law Council has detailed in this submission what it considers to be the key issues with the framework introduced by the TOLA Act:

    - the definition of 'serious Australian offences' and 'serious foreign offences';
    - the definition of 'systemic weakness' and 'systemic vulnerability';
    - the non-binding nature of the report and assessment by an expert former judge on the decision of the Attorney-General to issue a technical capability notice (**TCN**);
    - the absence of judicial approval for industry assistance notices;
    - computer access warrants permitting telecommunications interceptions under emergency authorisations;
    - the interaction of the TOLA Act with foreign laws; and
    - the capacity for reporting by the Commonwealth Ombudsman (**Ombudsman**) and the Inspector-General of Intelligence and Security (**IGIS**).

[1] This referral to the Independent National Security Legislation Monitor (**I**NSLM) was one of the recommendations set out in the Advisory Report of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) following the review by the PJCIS into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA) Act. See Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (Advisory Report, April 2019).

Background

6. The Law Council notes that when the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**the Bill**) was first introduced, it was referred to the Committee who tabled a report on 5 December 2018.[2] In response to the recommendations contained in that report, a number of amendments were introduced by the Government. One such amendment required the referral of the TOLA Act to the Committee for further review and inquiry, with the Advisory Report of the Committee issued in April 2019.

7. The April 2019 Advisory Report of the Committee focussed on 'clarifying the intent of the recommendations made in its 2018 Report and advising the Parliament on the extent to which those recommendations were addressed'.[3] The Committee stated that, given the timing of the then approaching federal election and the further statutory review now being undertaken by the Committee, it did not to seek to respond to the matters raised in the submissions and evidence given by stakeholders.[4]

8. Further amendments were made in February 2019. These amendments reintroduced the Australian Commission for Law Enforcement Integrity (**ACLEI**) and State and Territory independent commissions against corruption to the list of agencies deemed to be an 'interception agency' for the purpose of Part 15 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) and enabled the INSLM to review the TOLA Act.[5]

9. The Law Council acknowledges that the Government amendments to the Bill made some of the necessary improvements to the regime. In particular, there have been improvements to record-keeping, inspection and reporting requirements, and further accountability and oversight measures have been introduced.[6] However, further reforms are required to ensure the laws achieve a reasonable and proportionate approach to encrypted data in order to detect and respond to serious criminal activity.

Context and broad concerns

10. While much of the Law Council's submission is focussed on specific aspects of the TOLA Act and recommendations for its improvement, it is important to acknowledge the broader purposes of the scheme.

11. A principal objective of the TOLA Act is to increase public safety by providing faster access to encrypted data. The Law Council's comments endeavour to balance achievement of that objective with the need to ensure legislative clarity and certainty, particularly given the diverse range of agencies that may utilise these powers and the significant expansion in the range and nature of entities that will be relevantly subject to complex law enforcement legislation for the first time.

---

[2] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018).
[3] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Advisory Report, April 2019).
[4] Ibid 4 [1.17].
[5] Telecommunications and Other Legislation (Miscellaneous Amendments) Bill 2019 sch 1 item 1.
[6] For a complete list of what the Law Council considers to be the improvements made to the Bill by Government amendments to date, see 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) pp 8-11.

12. Measures introduced by the TOLA Act were developed to address threats by terrorists, child sex offenders and criminal organisations who use encryption and other forms of electronic protection to mask illegal conduct.[7] The TOLA Act was designed to address these threats by introducing a framework that improves the ability of agencies to access human-readable communications content and data.

13. However, the proposed measures go far beyond these threats by including lesser unlawful acts such as assisting the enforcement of any criminal law in force in any foreign country and enforcing laws imposing a pecuniary penalty thereby encompassing many, if not most, laws, including local government authority and council by-laws. In addition, extension of the measures includes exercise of a law enforcement power in relation to a matter 'that facilitates, or is ancillary and incidental to', such lesser unlawful acts.

14. Further, the current decision-making criteria within the TOLA Act do not task the relevant decision-maker, when making a 'reasonable and proportionate' determination on a matter, to examine whether perceived imperatives of law enforcement agencies outweigh reasonable expectations of confidentiality in electronic communications. Indeed, the TOLA Act does not specifically acknowledge that individuals and businesses are entitled to any reasonable expectation of confidentiality in communications. Nor does it acknowledge that overriding this expectation may adversely affect the trust of citizens and businesses in Australia as a reliably secure place to conduct business online.

15. The Law Council also notes that except for TCNs, the measures introduced by the TOLA Act are not subject to any form of consideration by an independent judicial officer. There should be *ex ante* review by an independent judicial officer in the case of Technical Assistance Requests (**TARs**) and Technical Assistance Notices (**TANs**).

16. In the absence of independent judicial review, and little transparency as to the frequency and nature of the use of these measures, there is a risk that the scheme created by the TOLA Act, which allows for exposure of such a broad range of private, domestic, commercial-in-confidence and sensitive communications for investigation of lesser offences, will both erode social licence for existence and use of such powers and undermine the reasonable expectations of confidentiality.

17. The Law Council's concerns are compounded by three further aspects of the TOLA Act:

    (a) the secrecy provision contained in section 317ZF of the Telecommunications Act is extraordinarily broad and effectively precludes effective engagement and consultation between a recipient organisation. The provision therefore precludes reasonable and appropriate transparency as to the exercise of these measures;

    (b) recipient organisations that are operating outside Australia (who may have a tenuous nexus to Australia) and are subject to foreign laws which preclude response to exercise of these measures are not afforded any defence to compliance with notices issued under the Telecommunications Act. The safe harbour provision under subsection 317ZB(5) is only in relation to legal proceedings for imposition of a civil penalty order. That is, the safe harbour is only in respect of the imposition of a financial penalty for committing an offence. It is not a safe harbour from exposure to criminal conviction; and

[7] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2.

(c) the computer access warrant powers represented a significant expansion of the current powers of law enforcement and the Australian Intelligence Security Organisation (**ASIO**).

Specific recommendations

18. The Law Council provides the INSLM with the following key recommendations in relation to: (a) industry assistance notices; (b) computer access warrants; and (c) voluntary and compulsory assistance to ASIO.

Recommendations for industry assistance notices

- The definition of 'serious offences' should be made consistent with the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), that is, punishable by a maximum term of imprisonment of seven years or more, not the currently prescribed three years.[8]

- The 'reasonable and proportionate' test within the Telecommunications Act should specifically require the decision maker to determine whether perceived law enforcement imperatives demonstrably outweigh the reasonable expectation of confidentiality in electronic communications between individuals and businesses.

- The list of 'acts and things' at subsection 317G(6) should be amended to replace the words '(but are not limited to)' with 'must be', as has been done for subsections 317L(3) and 317T(7).

- Any addition to an act or thing required under a TCN should be by legislative amendment. Alternatively, if it is to remain by legislative instrument, subsection 317T(6) should be amended so that the minister is required to explicitly consider the potential impact on human rights, such as the right to privacy.

- Disclosure of TAR, TAN or TCN information to the Office of the Australian Information Commissioner (**OAIC**) and the ACLEI should be deemed an authorised disclosure under subsection 317ZF(3).

- There should be 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 should be amended so that a request for disclosure from a 'Designated Communications Provider' (**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.

- Subsection 317ZG(1) should be amended to prohibit an industry assistance notice from requesting or requiring anything that might require a DCP to either implement or build any weakness or vulnerability into a current or proposed product or service.

- If the current definitions of 'systemic weakness' and 'systemic vulnerability' remain, the terms 'whole class of technology' and 'connected' should be clearly defined.

- 'Unauthorised third party' should be defined in section 317ZG in the following terms:

[8] *Telecommunications (Interception and Access) Act 1979* (Cth) s 5(2)(a).

- *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 at section 317ZG in the following terms:
  - *A reference to the information of, about or relating directly or indirectly 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 current time-limits contained in subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) regarding the extension and variation of TANs and TCNs should also apply to the extension and variation of TARs.

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

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

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

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

- The 'reasonable and proportionate' criteria should include a broader 'less intrusive' or 'less restrictive' test than that is currently provided by the Telecommunications 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 within the Telecommunications Act should 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';
  - include a higher threshold of 'significant or serious' national security and law enforcement interests at paragraphs 317JC(a)–(b), 317RA(a)–(b), 317ZAA(a)–(b) to;
  - specify that the 'legitimate interests of the DCP to whom the notice relates' include commercial interests at paragraphs 317JC(c), 317RA(g), 317ZAA(c) to;
  - omit from 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 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.[9]

- Decisions made under Part 15 of the Telecommunications Act should be made by a judicial officer. In the alternative, it recommended that judicial review of Part 15 decisions should be available.

- Section 317TAAA should be amended so that the Minister, when considering whether to approve the issuance of a TCN, is required to apply the decision-making criteria 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.

- Section 317LA should be amended to require the Australian Federal Police (**AFP**) Commissioner to not approve the issuance of a TAN unless satisfied of the matters specified in section 317P. Alternatively, section 317LA should be amended to expressly state the consultative and coordination role of the AFP Commissioner.

- The Telecommunications Act should 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 redaction power contained at subsection 317ZRB(7) of the Telecommunications Act relating to an Ombudsman’s report should be removed.

Recommendations for computer access warrants

- Section 32 of the *Surveillance Devices Act 2004* (Cth) (**SDA**) should be amended to state that telecommunications intercepts will not be permitted under emergency authorisations, consistent with the former subsection 32(4) of the SDA.

- The temporary removal power at section 25A of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) should be limited to the purpose of obtaining access to ‘relevant data’ under paragraphs 25A(4)(a), (ab) and 27E(2)(c) and (d) of the ASIO Act and 27E(2)(c) of the SDA.

[9] 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].

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

- The ASIO Act and the SDA should 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 section 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'.

- The ASIO Act and the SDA should 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.

Recommendations for assistance to ASIO

- Section 94 of the ASIO Act should be amended to require the Director-General to include in its annual report the kinds of circumstances in which voluntary assistance to ASIO (under paragraph 21A(1)(a)), and compulsory orders (under subsection 34AAA(2)), are being requested.
- Where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.
- Where a person is detained by ASIO in relation to an assistance order under section 34AAA of the ASIO Act, there should be minimum safeguards in place, including:
    - allowing the person to contact a lawyer or family member, where in the former case client confidentiality is preserved;
    - prescribing a maximum period for the giving of assistance;
    - requiring officers to explain the nature of the order, complaint mechanisms of the IGIS or how to challenge the order in a court;
    - requiring an interpreter if necessary; and
    - requiring that the person is treated humanely and with respect for their human dignity.

Schedule 1- Industry Assistance Notices

19. Schedule 1 is designed to promote cooperation between providers in the communications supply chain, and national security and law enforcement agencies. The Schedule creates levels of assistance for industry, ranging from voluntary assistance under a TAR through to mandated levels of cooperation under a TAN or TCN. The Law Council raises a number of concerns with the thresholds and oversight of this scheme set out in Schedule 1.

'Serious' offences

20. The industry assistance measures at Part 15 of the Telecommunications Act (introduced by Schedule 1 of the TOLA Act) apply to the investigation and prosecution of 'serious Australian offences' and 'serious foreign offences.' These terms were introduced to the Telecommunications Act by the TOLA Act, which inserted the following definitions:

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.*[10]

21. The effect of these amendments is that the powers set out in Part 15 of the Telecommunications Act, in particular, the power to issue a TAR, TAN or TCN[11] can be used in relation to a Commonwealth, State or Territory offence punishable by a maximum term of imprisonment of 3 years or more, or for life.

22. While this amendment appears consistent with the Committee's recommendation from its 2018 Advisory Report on the Bill,[12] the Law Council remains of the view that the threshold for the application of the powers in Part 15 of the Telecommunications Act remains too low. The Part 15 powers were intended to target the investigation of offences relating to terrorism or child exploitation[13], however the current definitions vastly expand the number of applicable offences and could be used against individuals suspected of committing relatively minor criminal offences.

Recommendation:

- **The definition of 'serious offences' should be made consistent with the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), that is, punishable by a maximum term of imprisonment of seven years or more, not the currently prescribed three years.**

Investigation or enforcement of laws ancillary to serious offences

23. Determination of whether use of the measures under the TOLA Act will be 'reasonable and proportionate' is in respect of a particular investigation of any of a broad range of acts, and ancillary activities. As noted above, the determination is act and offence specific, and not within the broader context of the appropriate balancing of societal interests.

24. The existing decision-making criteria does not task the relevant decision-maker, when making a 'reasonable and proportionate' determination, to balance law enforcement imperatives with the reasonable expectation held by individuals and businesses that electronic communications are secure from interference by authorities.

25. In the Law Council's view, the 'reasonable and proportionate' test within the Telecommunications Act should specifically require the decision-maker to determine whether perceived law enforcement imperatives demonstrably outweigh the reasonable expectation of confidentiality in electronic communications between individuals and businesses.

---

[10] *Telecommunications Act 1997* (Cth) s 317B definition of 'serious Australian offence' and 'serious foreign offence'.
[11] Ibid ss 317G, 317L, 317T.
[12] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) ix [2.3].
[13] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 2 [4]; [13] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 7 [7].

Recommendation:

- **The 'reasonable and proportionate' test within the Telecommunications Act should specifically require the decision-maker to determine whether perceived law enforcement imperatives demonstrably outweigh the reasonable expectation of confidentiality in electronic communications between individuals and businesses.**

Listed 'acts or things'

Exhaustive list of 'acts or things'

26. The TOLA Act introduced subsections 317G(6), 317L(3) and 317T(7) of the Telecommunications Act which provides 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.

27. In the Law Council's submission to the Committee's inquiry into the Bill, 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). The Committee also recommended in its report on the Bill that the definition of 'listed acts or things be exhaustive.'[14]

28. Subsequent 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. 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 remains non-exhaustive.

Recommendation:

- **The list of 'acts and things' at subsection 317G(6) should be amended to replace the words '(but are not limited to)' with 'must be', as has been done for subsections 317L(3) and 317T(7).**

Determination of listed acts or things for TCNs by legislation instrument

29. The Law Council notes that under subsection 317T(5), the Minister may, by legislative instrument, determine one or more kinds of acts or things, in addition to the listed acts or things under section 317E as it relates to TCNs. In making a determination, the Minister must have regard to the interests of law enforcement, the interests of national security, the objects of the Telecommunications Act, the likely impact on the determination on designated communications providers, and such other matters (if any) as the Minister considers relevant.[15]

30. The Law Council remains concerned that the ability for the Minister to make a determination via legislative instrument for an act or thing required under a TCN lacks appropriate oversight and should instead occur via legislative amendment. Alternatively, if it is to remain by legislative instrument, subsection 317T(6) should be amended so that the Minister is required to explicitly consider the potential impact on human rights, such as the right to privacy.

[14] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) xi [2.11].
[15] *Telecommunications Act 1997* (Cth) s 317T(6).

Recommendation:

- **Any addition to an act or thing required under a TCN should be by legislative amendment. Alternatively, if it is to remain by legislative instrument, subsection 317T(6) should be amended so that the Minister is required to explicitly consider the potential impact on human rights, such as the right to privacy.**

Unauthorised disclosure of information

31. Subsection 317ZF(1) 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 that the TOLA 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'.[16]

32. However, the Law Council maintains its position that disclosure of TAR, TAN or TCN information to the OAIC and ACLEI should be an authorised disclosure under section 317ZF(3),[17] as is provided for in paragraphs 122.5(3)(a)(ii) and (iii) of the *Criminal Code Act 1995* (Cth) (**Criminal Code**) as introduced by the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (**EFI Act**). Furthermore, the Law Council submits that the Telecommunications Act should be amended to provide for a defence to the unauthorised disclosure of information in accordance with the PID Act or the FOI Act, as is contained in the EFI Act.[18]

33. In the absence of these changes, a DCP, or an employee of a DCP that discloses 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), would have committed an offence under subsection 317ZF(1), which carries a penalty of five years imprisonments. The DCP, or the employee, would not have available a defence, for example, that the disclosure was in the public interest.

Recommendations:

- **Disclosure of TAR, TAN or TCN information to the OAIC and the ACLEI should be deemed an authorised disclosure under subsection 317ZF(3).**
- **There should be a defence to the unauthorised disclosure of information in accordance with the PID Act or the FOI Act.**

Expansion of authorised disclosures

34. The Government amendments improved section 317ZF by expanding the instances in which disclosure of information regarding TARs, TANs and TCNs is 'authorised' under section 317ZF, which now includes disclosure to a State or Territory inspecting body.[19]

35. This amendment appears to be consistent with the Committee's recommendation in its 2018 report on the Bill that it include 'express notification requirements and information

[16] Ibid s 317ZF(5A).
[17] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (18 October 2018) 32-3 [92]-[98].
[18] *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) s 122.5(4).
[19] *Telecommunications Act 1997* (Cth) ss 317ZF(5B)–(5C).

sharing provisions which would complement the inspection activities of State and Territory oversight bodies'.[20]

36. However, the Law Council considers that the authorised disclosure regime is 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.

37. 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 formal request for authorisation under subsections 317ZG(14)–(16). The Telecommunications Act grants broad discretionary powers regarding the decision of whether to grant a request for authorised disclosure, however, does not provide any indication of the circumstances in which an information disclosure request should or should not be authorised.

38. The Law Council supports an amendment to section 317ZF to the effect 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.[21] This would be consistent with earlier recommendations of the Committee.[22]

Recommendation:

- **Section 317ZF should be amended to the effect 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.**

'Systemic weakness' and 'systemic vulnerability'

39. 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.[23]

40. The Government amendments introduced a non-exhaustive definition of 'electronic protection' into the Telecommunications Act.[24] 'Electronic protection' now 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'.[25]

---

[20] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) x [2.6].
[21] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8625 proposed amendment (7).
[22] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) xiii [2.14].
[23] *Telecommunications Act 1997* (Cth) s 317ZG(1).
[24] Ibid s 317B definition of 'electronic protection'.
[25] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 10 [11].

Definition of 'systemic weakness' and 'systemic vulnerability'

41. The Law Council notes the following definitions 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.*[26]

42. The Law Council does not support these definitions of 'systemic weakness' and 'systemic vulnerability' on the basis that they 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 vague standard to meet 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.

43. Further, it is noted that the term 'whole class of technology' in the above definitions is not defined. The Supplementary Explanatory Memorandum to the TOLA Act provides some explanation regarding the intended meaning of 'whole class of technology', stating 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 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*.[27]

44. By contrast, the term 'target technology' is defined in the Telecommunications Act as introduced by the TOLA Act.[28] 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;

---

[26] *Telecommunications Act 1997* (Cth) s 317B definition of 'systemic weakness' and 'systemic vulnerability'.
[27] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 15 [51].
[28] *Telecommunications Act 1997* (Cth) s 317B definition of 'target technology'.

(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) 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.[29]

45. The Supplementary Explanatory Memorandum to the TOLA Act states in relation to 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 weakness or vulnerability in a particular service, device or item or software on a case-by-case basis.*[30]

46. The Law Council has previously recommended that subsection 317ZG(1) be amended so that 'electronic protection' be replaced by 'current or proposed product or service'.[31] 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.[32]

47. It appears that the Law Council's concerns remain in that subsection 317ZG(1) would operate to allow TARs, TANs and TCNs to introduce a weakness or a vulnerability into software or hardware[33] and carriage and electronic services.[34] 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. While the Telecommunications Act does not provide a definition or explanation of 'connected', the Supplementary Explanatory Memorandum to the TOLA Act provides some explanation:

> *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*.[35]

48. 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

---

[29] Ibid.
[30] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 16-7 [55].
[31] 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].
[32] Ibid.
[33] *Telecommunications Act 1997* (Cth) s 317B definition of 'target technology (c), (d)'.
[34] Ibid s 317B definition of 'target technology (a), (b)'.
[35] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 16 [52].

the introduction of a weakness or vulnerability, very wide. The Law Council is unsure as to how the term 'connected' in the Telecommunications 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 Telecommunications Act.

49. The Law Council maintains its position that the Telecommunications 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.

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

51. The Law Council regards the meaning of the 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, the law must be both readily known and available, and certain and clear, which includes the requirement that key terms should be defined.[36]

Recommendations:

- **Subsection 317ZG(1) should be amended to prohibit an industry assistance notice from requesting or requiring anything that might require a DCP to either implement or build any weakness or vulnerability into a current or proposed product or service.**
- **If the current definitions of 'systemic weakness' and 'systemic vulnerability' remain, the terms 'whole class of technology' and 'connected' should be clearly defined.**

Safeguards to protect against unauthorised third-party access

52. 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 any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.

53. 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.

54. The Law Council holds the view that clarity and certainty should be added to these safeguards.

[36] Law Council of Australia, *Policy Statement on Rule of Law Principles* (March 2011), 2 Principle 1(b).

Recommendation:

- **The term 'unauthorised third party' should be defined for the purposes of section 317ZG as including a reference to:**

  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.

55. Further, the Law Council notes the previously proposed amendment that 'otherwise secure information' should be defined in section 317ZG in the following terms:

> *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*.

56. 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.

Recommendation:

- **The term 'otherwise secure information' should be defined at section 317ZG as follows:**

  A reference to the information of, about or relating directly or indirectly 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.

Duration of TARs, TANs and TCNs

57. The TOLA Act includes 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.[37] 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 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.[38]

[37] *Telecommunications Act 1997* (Cth) ss 317MA(1C)–(1D), 317TA(1C)–(1D).
[38] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) x [2.7].

58. However, this time-limit does not apply to TARs. The Law Council is of the view that the time-limits as contained in subsections 317MA(1C)–(1D), 317TA(1C)–(1D), 317Q(11) and 317X(5) should also apply to the extension and variation of TARs.

59. Furthermore, it appears that amendments to the Telecommunications Act to date have not adopted the Law Council 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 view that the extension provisions should place a limit on the number of fresh notices that can be issued.

60. As noted above, the extension of a TAN or TCN requires the agreement of the DCP.[39] The Telecommunications Act should make it expressly clear that a notice can only be extended with the agreement of DCPs and not otherwise. The Law Council recommends that subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) be amended to include an express obligation on issuing agencies to inform DCPs of their right to refuse an extension, particularly at the point when a request for extension is pending.

Recommendations:

- **The current time-limits contained in subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) regarding the extension and variation of TANs and TCNs should also apply to the extension and variation of TARs.**
- **Sections 317HA, 317HA and 317TA should be amended to include a limit on the number of fresh notices or requests that can be issued.**
- **Subsections 317MA(1C)–(1D) and 317TA(1C)–(1D) should be amended to include an obligation on those seeking to extend a TAN or TCN to inform DCPs of their right to refuse the extension.**

Consultation requirements

61. The TOLA Act 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.[40] However, they are not required to consult the DCP if satisfied that the TAN should be given as a matter of urgency, or if the DCP has waived the duty to consult.[41]

62. 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.[42]

63. The Supplementary Explanatory Memorandum to the TOLA Act 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*

[39] *Telecommunications Act 1997* (Cth) ss 317MA(1C)–(1D), 317TA(1C)–(1D).
[40] *Telecommunications Act 1997* (Cth) s 317PA(1).
[41] Ibid s 317PA(2)–(3).
[42] Ibid s 317XA.

prevent those systems which maintain the security of personal information from being undermined.[43]

64. However, the Law Council is concerned that the effect of subsections 317W(7) and (8) could be that a replacement TCN, which effectively has the same requirements as a previous TCN, could be given to a DCP without its consent. Subsection 317W(7) provides that subsection 317W(1) does not apply to a TCN 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, there is no requirement for the DCP to be given written notice.

65. Subsection 317W(8) provides 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 new TCN is to come into force immediately after the expiry of the old TCN, the Attorney-General must consult the provider.

66. 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 only requirement on the Attorney-General is that it consult with the DCP.

67. Therefore, there could be the potential for a 'replacement' TCN 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. With this potential outcome in mind, the Law Council considers that the threshold in subsections 317W(7) and (8) of 'substantially the same' appears to be low and ambiguous.

68. 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 TOLA Act, 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.

69. The Law Council considers that the issuing agency should be required to obtain the consent for any extension or replacement of a TCN. If consent is not provided, 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 Telecommunications Act, regardless of how different or similar the requirements of the new TCN are compared to the requirements of a previous TCN.

Recommendation:

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

[43] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 10 [11].

Assessment by experts for TCNs

70. Subsection 317WA(1) permits 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;[44] 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.[45]

71. 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.[46]

72. 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.[47]

73. Section 317WA is consistent with the recommendation in the Committee's report on the Bill.[48] 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.[49]

74. The Law Council considers that the requirement that the Attorney-General consider the report, written by an expert and former judge in consideration of whether to proceed to give a TCN, is not sufficient. In order to ensure that this added layer of review and assessment of whether a TCN should be issued is objective and brings an external perspective to the decision-making, the Law Council recommends that the report of the

[44] *Telecommunications Act 1997* (Cth) s 317WA(4).
[45] Ibid s 317WA(5).
[46] Ibid s 317WA(7).
[47] Ibid s 317WA(6).
[48] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) xi-xii [2.12].
[49] *Telecommunications Act 1997* (Cth) s 317WA(11).

assessors be binding on the Attorney-General. That is, the Attorney-General must not proceed to give a TCN unless each assessor is satisfied with the matters set out in 317WA(7).[50]

Recommendation:

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

Decision-making criteria

75. The Law Council has welcomed the introduction of decision-making criteria to be applied in relation to the variation of TARs, TANs and TCNs.[51] The Law Council also supports amendments which have made it 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.[52]

76. While the Law Council supports the 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,[53] it considers that an express requirement of proportionality should be added to the decision-making criteria.

77. Subsection 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,[54] or of interest to the Australian Secret Intelligence Service (**ASIS**) or the Australian Signals Directorate (**ASD**) (TARs only),[55] are concerned.

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

79. 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.'[56] 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.

80. The Law Council recommends that the 'reasonable and proportionate' criteria should include a broader 'less intrusive' or 'less restrictive' test than that which is currently provided by the Telecommunications Act.

---

[50] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8625 proposed amendment (4), (6).
[51] Ibid ss 317JA(9)–(14), 317Q(10), 317X(4).
[52] Ibid ss 317JB(1A)–(3A), 317R, 317Z.
[53] Ibid ss 317JC(g), 317RA(eb), 317ZAA(eb); Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 10 [11].
[54] *Telecommunications Act 1997* (Cth) ss 317RA(ea)(i)–(ii), 317ZAA(ea)(i)–(ii).
[55] Ibid s 317JC(f).
[56] *Criminal Code Act 1995* (Cth) s 105A.12(4)(b).

Recommendation:

- **The 'reasonable and proportionate' criteria should include a broader 'less intrusive' or 'less restrictive' test and should relate to surveillance capabilities to obtain the information through other means – not simply through industry assistance.**

81. The Law Council further highlights its recommendations relating to the 'reasonable and proportionate' criteria that were contained in its earlier submissions to the Committee, including that the Telecommunications Act should 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) include a higher threshold of 'significant or serious' national security and law enforcement interests at paragraphs 317JC(a)–(b), 317RA(a)–(b), 317ZAA(a)–(b);

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

    (d) to omit from 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;

    (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.[57]

Accountability and oversight

Approval of industry assistance notices

Decisions to be made by a judicial officer

82. The Law Council maintains that the Telecommunications Act should be amended so that decisions made under Part 15 are made by a judicial officer. In the alternative, it recommended that judicial review of industry notice assistance decisions should be

[57] 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].

available.[58] 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.

83. While the TOLA Act introduced ministerial approval for TCNs, AFP Commissioner approval for TANs (see discussion below), and a former judge to take on a role in the decision-making process for a TCN,[59] there is no requirement for a judicial officer to be the primary decision maker for Part 15 industry assistance notices.

84. The Law Council supports the position that a TAN or TCN should not be issued or varied without the approval of an 'eligible judge'.[60] In the Law Council's view, an eligible judge should be required 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.[61]

Recommendation:

- **Decisions made under Part 15 of the Telecommunications Act should be made by a judicial officer. In the alternative, it is recommended that judicial review of Part 15 decisions should be available.**

Ministerial approval for TCNs

85. Amendments to the TOLA Act added a requirement that the Attorney-General must obtain approval from the Minister for Communications before the issuance of a TCN.[62] The Law Council supports this amendment, noting that it is 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'.[63]

86. However, when the Minister for Communications is considering whether to approve the issuance of a TCN, the decision-making criteria to which the Minister must have regard are far less extensive than the decision-making criteria in relation to a TAR or TAN.[64] These factors include:

---

[58] Ibid 21-2 [41]-[45], 31-2 [86]-[91].
[59] *Telecommunications Act 1997* (Cth) ss 317WA(4)–(5).
[60] 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 an 'eligible judge' would be a judge who is declared by the Minister to be an 'eligible judge' for the purposes of the Act.
[61] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8627 proposed amendment (5), (7) (for TANs), (10), (12) (for TCNs).
[62] *Telecommunications Act 1997* (Cth) s 317TAAA(1).
[63] 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) xi [2.9].
[64] *Telecommunications Act 1997* (Cth) s 317TAAA(6).

(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.

87. 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 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 Telecommunications 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.

88. As the Minister has the final say on whether a TCN will be given to a DCP, the Law Council suggests 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.

Recommendation:

- **Section 317TAAA should be amended so that the Minister, when considering whether to approve the issuance of a TCN, 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)

89. 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 under particular laws.[65] The Law Council supports these additions which seek to ensure that TARs, TANs and TCNs are not being used as a substitute for warrants or authorisations.

90. However, the Law Council notes paragraph 317ZH(1)(e) was omitted, effectively removing the *Intelligence Services Act 2001* (Cth) (**IS Act**) from the list of laws requiring a warrant process to be observed. The IS Act requires ASIS and the ASD to gain ministerial approval before, for example, undertaking activities for the purposes of producing intelligence on an Australian person.[66]

91. By omitting paragraph 317ZH(1)(e), a TAR, TAN or TCN would not be rendered invalid if it required a DCP to do any act or thing which would otherwise require ministerial approval under the IS Act.

[65] Ibid s 317ZH(1)-(3).
[66] *Intelligence Services Act 2001* (Cth) s 8(1)(a)(i).

92. The Supplementary Explanatory Memorandum states the reason for the removal is so that agencies under section 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.[67]

93. 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.

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

94. 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.

95. This 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.'[68]

96. However, the AFP Commissioner is not required to apply the same statutory criteria as if it were the original issuing body.[69] In fact, it is not required to apply any statutory criteria.

97. 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*.[70]

98. The Law Council notes that 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 statutory criteria, and go through the same decision-making process, as would apply if the AFP were the original issuing authority.[71] The Law Council is therefore supportive of an amendment which would require that the AFP Commissioner not to give approval for the issuance of a TAN unless satisfied of those matters specified in section 317P.[72]

---

[67] Ibid.
[68] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) ix [2.8].
[69] *Telecommunications Act 1997* (Cth) s 317P.
[70] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 25 [124].
[71] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) ix-x [2.5].
[72] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 8625 proposed amendment (2).

99. 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*.[73]

100. 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 specify this role for the AFP Commissioner.

Recommendation:

- **Section 317LA should be amended to require the AFP Commissioner to not give approval for the issuance of a TAN unless they are satisfied of the matters specified in section 317P. Alternatively, section 317LA should be amended to expressly state the consultative and coordination role of the AFP Commissioner.**

Notification requirements

101. 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,[74] variation[75] or revocation[76] of a TAR, TAN or TCN. These amendments to the TOLA 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.[77]

102. The TOLA Act 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.[78] If the chief officer of an interception agency gives a TAN to a DCP, they are under the same obligation 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.[79]

103. The Law Council considers the obligation to inform DCPs of their right to complain as a positive step. However, it is not clear why this obligation applies only to the issuance of a TAN, and not for all Part 15 industry assistance notices. The Law Council considers that the scheme should be amended so that any agencies issuing a TAR, TAN or TCN

---

[73] Supplementary Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 25 [124].
[74] *Telecommunications Act 1997* (Cth) ss 317HAB, 317MAB, 317TAB.
[75] Ibid ss 317JA(15)–(19), 317Q(12)–(14), 317X(6)–(8).
[76] Ibid ss 317JB(6)–(10), 317R(5)–(7), 317Z(3)–(5).
[77] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018) x [2.6].
[78] *Telecommunications Act 1997* (Cth) ss 317MAA(3).
[79] Ibid ss 317MAA(4).

are obliged to inform the DCP who is receiving the notice of its right to complain to the relevant overseeing or inspecting body.

Recommendation:

- **The Telecommunications Act should 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.**

Inspection by and reporting to the Ombudsman

104. The Law Council welcomes the amendments relating to 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 when this occurs, the Home Affairs Minister must table the report in Parliament.[80]

105. 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.'

106. While the Law Council supports the introduction of this inspection measure, 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.

107. The Law Council further 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.[81]

108. 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 to remove the redaction power contained at subsection 317ZRB(7) of the Telecommunications Act.[82]

Recommendation:

- **The redaction power contained at subsection 317ZRB(7) of the Telecommunications Act relating to an Ombudsman's report should be removed.**

---

[80] Ibid ss 317ZRB(4), (6).
[81] *Telecommunications Act 1997* (Cth) s 317ZRB(7).
[82] 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.

Adequate resources for effective oversight

109. The Law Council notes and supports the recommendation of the Committee in its review of the TOLA Act that the Government continues to ensure that the IGIS and the Ombudsman have sufficient resources 'to ensure they can properly execute their additional responsibilities under the Assistance and Access Act'.[83]

110. The Law Council notes the Government response, as tabled in the Senate on the 17 September 2019, that the Governments supports this recommendation and will monitor impacts of the TOLA Act on both the IGIS and the Ombudsman and consider additional resourcing. The Law Council considers that the additional resourcing is an essential component of effective oversight and accountability measures relating to the TOLA Act and they should be allocated as a matter of urgency.

Schedule 2 - Computer Access Warrants

111. Schedule 2 enables federal, State and Territory law enforcement agencies to obtain covert computer access warrants when investigating specific Commonwealth offences. The Law Council has some concern with the scope of these provisions, and the degree to which appropriate safeguards are in place.

Emergency authorisations

112. 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 paragraph 27E(2)(h) of the SDA, a computer access warrant would allow agencies to intercept communications over a telecommunications system.

113. This is a shift from 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]'.

114. The Law Council has noted that attaching telecommunications interception power to computer access warrants involves a reduction in the threshold for telecommunications interception.[84] 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 likely to be obtained by interception 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.[85] As noted above, serious offences generally include offences punishable by imprisonment for life or for a period or a maximum period of at least seven years under section 5D of the TIA Act.

115. 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

[83] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, 3 April 2019) xi.
[84] Ibid.
[85] *Telecommunications Act (Interception and Access) Act 1979* (Cth) s 46(1)(d).

Judge or a nominated AAT member, and these warrants can be issued for a much broader range of offences.

116. The Law Council therefore is of the view that section 32 of the SDA should 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.[86]

Recommendation:

- **Section 32 of the SDA should be amended to state that telecommunications interception will not be permitted under emergency authorisations, consistent with the former subsection 32(4) of the SDA.**

Removal of computer or other things from premises

117. The Law Council reiterates its concern that the temporary removal of computers and other things pursuant to section 25A of the ASIO Act and section 27E of the SDA is too broad.[87] It allows the Attorney-General, 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.[88] It is unclear why this power is necessary or justified.

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

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

120. The TOLA Act introduced 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[89] or authorisation,[90] 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.

121. 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.

122. The Law Council recommends that subsections 25A(4A), 27E(3A) and 27E(2A) of the ASIO Act be amended to introduce a quantifiable time-limit for the return of

---

[86] 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].
[87] Ibid 41-2 [122]-[127].
[88] *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).
[89] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4A), 27E(2A).
[90] Ibid s 27E(3A).

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.

Recommendations:

- **The temporary removal power at section 25A of the ASIO Act should be limited to the purpose of obtaining access to 'relevant data' under paragraphs 25A(4)(a), (ab) and 27E(2)(c) and (d) of the ASIO Act and 27E(2)(c) of the SDA.**
- **Subsections 25A(4A), 27E(3A) and 27E(2A) of the ASIO Act should be amended to introduce a quantified time-limit for the return of computers, and a requirement that the removal or retention of a computer for any time after the prescribed time-limit must only occur following an approved extension from a court.**

Concealment of access

123. Subsections 25A(8), 27A(3C) and 27E(6) of the ASIO Act and paragraphs 27E(7) of the SDA authorise specified concealment activities while a 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.

124. The Law Council has concerns regarding the automatic authorisation of concealment activities, and the absence of a time-limit by which concealment of access powers may be exercised.[91] Neither of these issues have been resolved.

125. The Law Council considers 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. At the time, the Law Council 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 was 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.

126. The TOLA Act 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 request an extension of time from the Attorney-General. Rather, the TOLA Act inserted section 49B in the SDA, which requires that the Ombudsman is notified when an act or thing is done

[91] 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].

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 were done.

127. 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.

Recommendation:

- **The ASIO Act and the SDA should 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

128. The TOLA Act 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.

129. These provisions seek to provide limitations on any damage or loss caused by the concealment activities, which assists in the proportionality of the measures, and are consistent with other provisions in the ASIO Act which refer to 'material loss or damage'.

130. However, the loss or damage caused must 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. The Law Council therefore recommends that these sections be amended to omit the requirement of 'material'.

Recommendation:

- **Subsections 25A(9) and section 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'.**

Authorised disclosures

131. The Government amendments improved 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.[92]

[92] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 23AB(3)–(5), 63AC(3)–(5).

132. In relation to disclosures in the context of obtaining legal advice, 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.

133. However, 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. 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.

134. Similarly, Division 1 of Part 6 of the SDA relates to restrictions on use, communication and publication of information. Paragraph 44(1)(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 publicise 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 proceedings 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.

135. Noting the above, the Law Council is of the view that the ASIO Act and the SDA should 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.

Recommendation:

- **The ASIO Act and the SDA should 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 – Australian Security Intelligence Organisation

136. Schedule 5 of the TOLA Act enables ASIO to compel a person to provide assistance in accessing data held on a device. It also provides that where a person has voluntarily provided ASIO assistance, they may be conferred immunity from civil liability associated with that assistance. In relation to the operation of Schedule 5, the Law Council raises the following concerns.

Voluntary assistance to ASIO

Civil immunities for voluntary assistance to ASIO

137. 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.

138. The Law Council 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; and

(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;

(f) and the extent to which the civil immunity provision did not apply.

139. The TOLA Act 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.[93] 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 clarifying the responsibilities for ASIO.

140. 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.[94] 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.

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

141. In relation to point (f) above, subsection 94(2BC) was introduced into section 94 of the ASIO Act by the TOLA Act. This subsection requires the annual report, prepared by the Director-General of Security for the Minister,[95] include a statement of the total number of requests made under paragraph 21A(1)(a) during the period,[96] as well as the total number of orders made under subsection 34AAA(2) during the period.[97]

142. 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.

143. However, this amendment may not be sufficient 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 TOLA Act introduced paragraph 317ZS(1)(d), which requires the Home Affairs Minister 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 provided to Parliament.[98]

144. 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.

Recommendation:

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

Ministerial oversight

145. The Law Council is concerned about the potential for ASIO to request voluntary assistance avoiding the need to otherwise obtain special powers warrants that would require Ministerial authorisation under the ASIO Act. This may create a risk that an aggrieved person will not have access to a legally enforceable remedy given the availability of the immunity of civil liability. It would also reduce the safeguards involved in requiring ASIO to obtain Ministerial approval. The Law Council considers that where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.

Recommendation:

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

[95] *Public Governance, Performance and Accountability Act 2013* (Cth) s 46.
[96] *Australian Security Intelligence Organisation Act 1979* (Cth) s 94(2BC)(a).
[97] Ibid s 94(2BC)(b).
[98] *Telecommunications (Interception and Access) Act 1979* (Cth) s 186(3).

Compulsory assistance to ASIO

Procedural matters

146. The Government amendments to the TOLA Act 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.[99]

147. Instructions for the cessation of activities are present in the TOLA Act. Subsections 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.

148. 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. However, as set out below, there are outstanding issues relating to the detention for non-compliance with the order and the lack of requirements to guard against oppressive use of multiple coercive powers to obtain particular information.

Complying with an order amounting to detention

149. If a person is required to attend a place to provide information or assistance to ASIO under a section 34AAA, this may arguably amount to detention of the person, particularly as they may be arrested on suspicion of the offence in subsection 34AAA(4) if they attempted to leave. There are little if any safeguards to guard against the risk that this may amount to arbitrary detention, particularly as the order is not made by a judicial officer.

150. The current questioning warrants and questioning and detention warrants under Part III, Division 3 of the ASIO Act contain more safeguards than that proposed for the new orders. If the possibility for detention is to remain, the Law Council suggests the scheme should be amended to guarantee a range of minimum safeguards.

Recommendation:

- **Where a person is detained by ASIO in relation to an assistance order under section 34AAA of the ASIO Act, there should be minimum safeguards in place, including:**
  - **allowing the person to contact a lawyer or family member, where in the former case client confidentiality is preserved;**
  - **prescribing a maximum period for the giving of assistance;**
  - **requiring officers to explain the nature of the order, complaint mechanisms of the IGIS or how to challenge the order in a court;**
  - **requiring an interpreter if necessary; and**
  - **requiring that the person is treated humanely and with respect for their human dignity.**

[99] *Australian Security Intelligence Organisation Act 1979* (Cth) s 34AAA(3A)–(3B).

Interaction with foreign laws

151. The Law Council considers it useful to comment on the interaction of the amendments introduced by the TOLA Act with foreign laws – in particular the United States *Clarifying Lawful Overseas Use of Data Act*[100] (**CLOUD Act**) and the European Union's (**EU**) *General Data Protection Regulation* (**GDPR**).[101]

Interaction with the United States CLOUD Act

152. 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.[102]

153. 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[103] in certain conditions.[104]

154. 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 AFP in certain circumstances.[105]

155. 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**).[106]

156. The CLOUD Act achieves this by amending the *Electronic Communications Privacy Act*[107] (**ECPA**) which regulates the US service provider's disclosure of information about their users, and previously precluded US providers from disclosing user's telecommunications data or communications content to foreign governments.

157. 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

---

[100] *Clarifying Lawful Overseas Use of Data Act,* HR 4943, 115th Congress (2017-2018).
[101] *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.
[102] *Consolidated Appropriations Act of 2018*, Pub L No 115-141, § 102, 132 Stat 1213.
[103] See *Microsoft Corp. v United States,* 829 F 3d 197, 210 (2d Cir, 2016).
[104] 18 USC § 2713.
[105] Ibid §§ 2702, 2703.
[106] 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.
[107] *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.[108]

158. 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 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.*[109]

159. 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'.[110]

160. 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'.[111]

161. 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.

162. 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*.[112]

163. Further, the amendments introduced by the TOLA 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 TOLA 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

[108] 18 USC § 2523(b)(1).
[109] Digital Industry Group Inc., Submission No 78 to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (19 October 2018) 3.
[110] 18 USC § 2523(b)(3).
[111] 18 USC § 2523(b).
[112] *Convention on Cybercrime*, opened for signature 23 November 2011, ETS No 185 (entered into force 1 July 2004).

authority prior to, or in proceedings regarding, enforcement of the order' and this condition may not be adequately addressed by the amendments introduced by the TOLA Act.

164. It could be argued that section 317ZH of the Telecommunications Act places a restriction on a TAN or a 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'.

165. However, the second, more problematic issue is the inconsistency of the obligations in relation to encryption imposed by the TOLA Act and the US federal law, contained in the *Communications Assistance for Law Enforcement Act 1994* (US) (**CALEA**).[113] The CALEA 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'.[114] 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"'.[115]

166. Irrespective of the amendments introduced by the TOLA 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 TOLA Act.

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

168. The Law Council maintains that with the exception of the procedure to issue a TCN, the other measures introduced by the TOLA Act are not subject to any form of consideration by an independent judicial officer, notwithstanding the 'general limits' provided by section 317ZH of the Telecommunications 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.

169. 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 TAR,[116] there is no provision for the judicial review of the actual decision to issue the TAN, TCN or TAR.

---

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

Interaction with the laws of the European Union

170. The EU's GDPR commenced on 25 May 2018. The GDPR sets a number of restrictions on the processing and transfer of 'personal data'[117] 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[118]; 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.[119]

171. 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.

172. 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.

173. 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 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.

174. While there is a defence under the TOLA 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,[120] 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.[121]

175. 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

---

[117] '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).
[118] Ibid art 3(1).
[119] Ibid art 3(2).
[120] *Telecommunications Act 1997* (Cth) s 317ZB(5).
[121] 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).

it only requires an employee to do an act or thing in Australia, the software is partially 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.

176. 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.

177. Personal data may possibly be released from the EU pursuant to an order issued under the TOLA 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'.[122] It may be that an argument could be made that a serious threat to Australian security would be 'important reasons of public interest'.[123]

178. 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.

The United Kingdom Scheme

179. The Law Council understands that the INSLM is interested in stakeholder views on the corresponding framework in the United Kingdom (**UK**), and whether there are elements of the UK model that could be integrated into the Australian context. The Law Council has engaged with this issue in further detail below.

The Judicial Commissioner

180. In 2016, the UK Government legislated to introduce a new scheme for the authorisation and review processes relating to the exercise of coercive powers available to law enforcement agencies through the enactment of the *Investigatory Powers Act 2016* (UK) (**IP Act**). These provisions extend to authorising the use of powers relating to the interference with telecommunications equipment to access encrypted telecommunications data though the issue of either a 'targeted equipment interference warrant'[124], 'national security notice' or a 'technical capability notice'.[125]

181. According to the UK Government's published information, the IP Act:

[122] *GDPR* art 49(1)(d).
[123] 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.
[124] *Investigatory Powers Act 2016* (UK) s 99.
[125] Ibid s 252.

Brings together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will make these powers and the safeguards that apply to them clear and understandable.[126]

182. Furthermore, the IP Act:

Radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these (and other warrants) cannot come into force until they have been approved by a judge. And it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used.[127]

183. The Law Council considers that is useful to have the additional safeguard of the 'double-lock' as applied in the UK. In that jurisdiction even where the warrant or notice is required to be issued urgently, it is still reviewed by and requires the subsequent approval of a 'Judicial Commissioner' to remain in force. This ensures that warrants and notices issued by the Secretary of State authorising the use of coercive powers must always be reviewed by an independent judicial authority, the 'Judicial Commissioner', who sits under the Investigatory Powers Commissioner (**IPC**), before the warrants can be issued and executed by the relevant investigatory agency.[128]

184. These coercive powers the scheme applies to includes:

(a) targeted interception, targeted examination of bulk telecommunications data and mutual assistance warrants (the equivalent of Australian telecommunications interception) and targeted examination warrants (relating to bulk telecommunications such as what is retained under the mandatory telecommunications data retention scheme in Australia);

(b) targeted equipment interference warrant or a 'national security notice' (the equivalent of the Australian TAN); and

(c) technical capability notices (which is like the Australian TCN).

185. The Secretary of State can only issue a warrant:

(a) if it is in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic wellbeing of the United Kingdom (so far as those interests are also relevant to the interests of national security); and

(b) if the Secretary of State believes that the activity set out in the warrant is proportionate to the intended outcome and if the Secretary of State considers that appropriate safeguards are in place.[129]

186. The IP Act provides for the appointment of the IPC and the Judicial Commissioners by the Prime Minister. It also provides that a person is not to be appointed as the IPC or another Judicial Commissioner unless the person holds or has held a high judicial

[126] UK Government, 'Investigatory Powers Act' (Web page, 18 December 2017) <https://www.gov.uk/government/collections/investigatory-powers-bill>.
[127] Explanatory Note, *Investigatory Powers Act 2016* (UK) (18 December 2017) <https://www.gov.uk/government/collections/investigatory-powers-bill>.
[128] *Investigatory Powers Act 2016* (UK) s 19.
[129] Ibid s 102.

office - referring to the same qualifications for appointment as a judge of the Supreme Court of the United Kingdom.

187. In considering whether to approve a decision to issue a warrant, a Judicial Commissioner must review the conclusions reached by the Secretary of State (or the equivalent Scottish Minister) regarding the necessity and proportionality of the warrant.[130] In doing so the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review.[131]

188. If a Judicial Commissioner refuses to approve a decision to issue a warrant, the agency who requested the warrant may ask the IPC to reconsider that application. However, should the IPC also refuse to approve the warrant there is no right of appeal and the warrant cannot be issued.

189. The Law Council maintains that requiring some independent judicial review of all the authorisations of TARs, TANs and a TCNs would assist in addressing the requirement of necessity and proportionality in the use of these powers. In doing so, it would hopefully also assist in restoring the trust of both the public and industry in the integrity of the scheme. A further advantageous implication of adopting a means for independent judicial review of the use of these powers is that it is likely to address the problems identified above in relation to how the amendments introduced by the TOLA Act interact with foreign laws and in particular, would assist Australia to be able to enter into an 'executive agreement' with the United States under the CLOUD Act.

190. As a general rule, the Law Council considers that there is merit in considering a consistent approach to the authorisation of coercive law enforcement powers in order to avoid overlapping laws which create confusion and misunderstanding of the use of coercive powers by law enforcement agencies. However, whether the model of a IP Act which applies to the authorisation of all coercive law enforcement powers, as adopted in the UK, is appropriate in the Australian context is a complex question, and one that may be considered by the current review being conducted in relation the legal framework of the national intelligence community.[132] However, the Law Council welcomes measures which would improve the proportionality of the amendments introduced by the TOLA scheme including the judicial review of authorisations to notices under the scheme that seek to compel industry assistance.

Technical Advisory Bodies

191. Under the IP Act there is provision for the establishment of two advisory bodies to assist both the Secretary of State and the IPC and Judicial Commissioners in the discharge of their powers to review the authorisation of the use of coercive powers as they relate to telecommunications data. Section 246 of the IP Act compels the IPC to ensure there is a 'Technical Advisory Panel' (**the Panel**) which is a statutory body established to provide advice to the IPC, the Secretary of State and the Scottish Ministers about:

(a) the impact of changing technology on the exercise of investigatory powers whose exercise is subject to review by the IPC; and

---

[130] *Investigatory Powers Act 2016* (UK) s 23.
[131] See, eg, *Investigatory Powers Act 2016* (UK) s 254.
[132] See Dennis Richardson AO, *Comprehensive Review of the Legal Framework Governing the National Intelligence Community* (30 May 2018) <https://www.ag.gov.au/NationalSecurity/Pages/Comprehensive-review-of-the-legal-framework-governing-the-national-intelligence-community.aspx>.

(b) the availability and development of techniques to use such powers while minimising interference with privacy.

192. The members of the Panel are appointed by the IPC under the IP Act. The Panel is in addition to the 'Technical Advisory Board' which is also a statutory body established under the IP Act and consists of members from both law enforcement and intelligence agencies, as well as the telecommunications industry.[133]

193. The Law Council considers that given the dynamic nature of innovation and change in the telecommunications and cyber industry, it would be of benefit to the scheme introduced by the TOLA Act to also have equivalent statutory bodies that can assist both the Attorney-General, and, if implemented, the responsible judicial reviewing authorities in understanding the competing needs of law enforcement agencies and the telecommunications and cyber industry. The provision of independent advice to an independent reviewing authority would be important to ensure that the authorisation for the use of the coercive powers is made with the requisite knowledge to make an informed decision based on current technology and industry practice.

[133] *Investigatory Powers Act 2016* (UK) s 247.