Law Council
OF AUSTRALIA

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Parliamentary Joint Committee on Intelligence and Security

18 October 2018

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 2018 Executive as at 1 January 2018 are:

- Mr Morry Bailes, President
- Mr Arthur Moses SC, President-Elect
- Mr Konrad de Kerloy, Treasurer
- Mr Tass Liveris, Executive Member
- Ms Pauline Wright, Executive Member
- Mr Geoff Bowyer, Executive Member

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

Acknowledgement

The Law Council acknowledges the assistance of its Privacy Law Committee of the Business Law Section, and its National Criminal Law Committee, in the preparation of this submission.

Executive Summary

1. The Law Council welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (**PJCIS**) inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**the Bill**).

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

3. A principal objective of the Bill 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:

   (a) that the proposed measures are reasonable, necessary and proportionate, including by incorporating reasonably transparent and verifiably reliable safeguards and controls; and

   (b) 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 subject to complex law enforcement and intelligence legislation for the first time.

4. In the timeframe available in which to prepare submissions to the inquiry, and given the length and complexity of the Bill, the Law Council has not been able to comprehensively examine the Bill. This submission highlights key concerns and suggestions for improvement that the Law Council has identified to date.

5. The Law Council considers that the Bill should only be passed if it is redrafted in a manner to ensure its operation is defined by what is reasonable, necessary and proportionate to ensure public safety. According to the Explanatory Memorandum, the Bill has been 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.[1] The Bill intends to address these threats by introducing a suite of measures that will improve the ability of agencies to access human-readable communications content and data.

6. In fact, the measures proposed go far beyond these threats, to include 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 (being many, if not most, laws, including local government authority and council by-laws).[2] In addition, the measures include exercise of a law enforcement power in relation to a matter 'that facilitates, or is ancillary and incidental to', such lesser unlawful acts.

---

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

[2] The Law Council notes that in each case the power would only be exercisable by an agency listed as an 'interception agency' in proposed section 317B, but this will include Federal, State and Territory Police Forces acting in aid of other Government agencies. The Law Council does not consider that involvement of a police force is of itself an adequate safeguard in itself against overly expansive use of this power in aid of other Government agencies.

7. Further, decision making as to possible exercise of a power in relation to a particular set of facts or allegations is not required to take into account the wider context of maintaining citizen trust as to these broad powers. The decision making criteria do not task the relevant decision maker, when making a 'reasonable and proportionate' determination, to determine whether perceived imperatives of law enforcement agencies should outweigh affected individuals' and businesses' reasonable expectations of confidentiality and privacy in communications. That is, decision making as to possible exercise of a power may be act and offence specific, not within the broader context of the appropriate balancing of societal interests and individual autonomy. Indeed, the Bill does not specifically acknowledge that individuals and businesses are entitled to any reasonable expectation of confidentiality in communications, and that overriding that expectation may adversely affect digital trust of citizens and businesses in Australia as a reliably secure place to conduct business.

8. The Bill confers an unstructured discretion upon the decision maker to determine whether the use of the measures is 'reasonable and proportionate' for investigation of an act (or ancillary activity) that is suspected to have occurred within any of a broad range of unlawful acts. The 'reasonable and proportionate' test should include 'necessity' and also specifically require the decision maker to determine whether possible exercise of a power is necessary to 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 citizens in confidentiality in communications between individuals and businesses and within businesses.

9. Except for technical capability notices (**TCNs**), the new measures are not subject to any form of consideration by an independent judicial officer. The Law Council submits that there should be *ex ante* decision making or review by an independent judicial officer in the case of requests and notices.

10. In the case of TCNs, there is a requirement for exercise of discretion by the Attorney-General. The Attorney-General is of course usually a well credentialed judicial officer, but the Attorney-General is not a demonstrably independent party.

11. Absence of independent judicial review, and little transparency as to the frequency and nature of use of these measures, there may be a risk that this Bill (if enacted in its current form) will result in erosion of digital trust of citizens in activities of intelligence and law enforcement agencies. In a social environment where trust in public institutions is at historical lows, there is a substantial risk that legislation which allows for exposure of a broad range of private, domestic, commercial-in-confidence and sensitive communications for investigation of lesser offences will erode social licence for existence and use of such powers to address threats by terrorists, child sex offenders and criminal organisations who use encryption and other forms of electronic protection to mask illegal conduct.

12. The Law Council's concerns as summarised in the previous paragraphs are compounded by three further aspects of the Bill. First, the secrecy provision (proposed section 317ZF) is extraordinarily broad and effectively precludes effective consultation by a recipient organisation and within a recipient organisation. The provision therefore precludes reasonable and appropriate transparency on the recipient side as to exercise of these measures. Second, recipient organisations operating outside Australia (which may have very tenuous nexus to Australia) and that are subject to foreign laws which preclude response to exercise of these measures are not afforded any defence in compliance with notices issued under this

Bill. The safe harbour under proposed 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, not a safe harbour from being found to have committed an offence. This creates potential reputational and financial risk and jeopardy for many organisations that are required to report as to their compliance with laws. Third, and as discussed in detail later in this submission, the computer access warrant powers represent a significant expansion of law enforcement and national security agencies' current powers.

13. The Law Council makes a number of recommendations aimed at improving the Bill to ensure that the measures, and the circumstances when those measures may be used, are reasonable, necessary and proportionate.

Improvements made on Exposure Draft and Ongoing Previous Law Council Recommendations

14. The Law Council notes that the PJCIS's Inquiry into the Bill follows a consultation conducted by the Department of Home Affairs (**Department**) on the Exposure Draft of the Bill, to which the Law Council provided a submission.[3] The Law Council refers that submission, which it has provided to the PJCIS, for its consideration.

15. The Law Council made a number of recommendations in the submission to the Department aimed at improving the legislation. The Law Council welcomes the following amendments to the Bill as responsive to its recommendations to the Department regarding the Exposure Draft of the Bill:

- proposed subsection 317ZB(5) of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) which provides that in proceedings for a civil penalty order against a designated services provider for a contravention of failing to comply with a technical assistance notice (**TAN**) or a TCN, where the TAN or TCN requires the provider to do an act or thing in a foreign country, it is a defence if the provider proves that compliance with the requirement in the foreign country would contravene a law of the foreign country. However, see the Law Council's comment above to the effect that this safe harbour should not only be in respect of imposition of a financial penalty for committing an offence, and should be a defence in relation to the offence); and
- the removal of 'protecting the public revenue' from the listed acts or things under proposed section 317E of the Telecommunications Act. This means that 'protecting the public revenue' is no longer a valid reason for a law enforcement or relevant intelligence agency to request a designated service provider to comply with a technical assistance request (**TAR**), TAN or TCN. However, this appears to be overridden by the broader concept of 'specified acts or things' as used in proposed subsection 317G(2), of which 'listed acts or things' appear to be a sub-set. The net effect appears to be that the measures may be exercised in relation to laws imposing pecuniary penalties that are laws to protect public revenue.

16. The Law Council supports proposed section 317W as an additional requirement now included in the Bill. This amendment inserts a requirement for the Attorney-General

[3] Law Council of Australia, Submission to the Department of Home Affairs, *Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* available online https://www.lawcouncil.asn.au/docs/6e0bcb0a-44bd-e811-93fc-005056be13b5/3504%20-%20Assistance%20and%20Access%20Bill%202018.pdf.

to consult with the designated communications provider before issuing a TCN. The effect of this provision is that the Attorney-General must consult with the provider by providing them with a written notice setting out a proposal to give a TCN and inviting the provider to make a submission regarding the proposed TCN. Proposed subsection 317W(7) would allow the Attorney-General and the provider to jointly appoint one or more persons to carry out an assessment of whether the proposed TCN would require a provider to implement or build a systemic weakness or vulnerability in contravention of proposed section 317ZG. The person appointed must have the knowledge that would enable them to assess whether a TCN would contravene proposed section 317ZG.[4] Further, under proposed subsections 317W(8)-(9) the designated communications provider must agree to be responsible for the remuneration of the person appointed, however the Commonwealth may reimburse the provider for the whole or part of the remuneration.[5] The Law Council supports this amendment to the Bill in order to provide further oversight over the process of issuing a TCN.

17. The Law Council maintains the following recommendations submitted to the Department that have not been addressed, for the reasons outlined in the original submission regarding the Exposure Draft Bill:[6]

- The Bill should be amended to ensure that powers in the Bill cannot be used to impose data retention capability or interception capability obligations, or to require provision of access to the content of a communication or electronic record where the recipient is a telecommunications carrier or a carriage service provider, are extended and apply to all designated communications providers (specifically including those designated communications providers that are not Australian telecommunications carriers or carriage service providers).
- The Bill should prohibit a TCN or TAN from requiring any act or omission that might require a designated communications provider to either implement or build any weakness or vulnerability into a current or proposed product or service.
- The Bill should be amended to limit the scope of application to companies with direct control and access to encrypted information.[7]
- The Bill should be amended to reflect the following:
  - Establishment of an upper limit for non-compliance fines, particularly for small businesses, in addition to the maximum established per case.
  - A clear explanation of how TCNs will apply to entities outside of Australia where the warrant giving the authority to issue the TCN does not apply.

[4] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 1 item 7, s 17W(8).
[5] Ibid s 317W(9)-317W(10).
[6] Law Council of Australia, Submission to the Department of Home Affairs, *Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* available online https://www.lawcouncil.asn.au/docs/6e0bcb0a-44bd-e811-93fc-005056be13b5/3504%20-%20Assistance%20and%20Access%20Bill%202018.pdf, 10-11.
[7] The Exposure Draft Bill allows the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate or interception agencies to issue TANs and TCNs. These notices can require a designated communications provider to undertake an extremely broad range of activities going beyond simply accessing encrypted data, including: installing, maintaining, testing or using software or equipment (proposed subsection 317E(c)); assisting with the testing, modification, development or maintenance of a technology or capability (proposed subsection 317E(f)); and modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider (proposed paragraph 317E(h)).

- Including in the requirements for practicability and technical feasibility, a requirement that the granting authority weigh the significance of the issue to which the warrant or authorisation relates with the economic impact on the party to whom the warrant or authorisation is being issued. A minor issue with significant compliance cost to the recipient that is a small business might not justify the granting of the warrant, whereas a more important issue might.
- Providing limits on the extent to which the bodies seeking the warrant or authorisation can transfer data filtering or data organisation tasks onto the recipient.

- For law enforcement agencies, the Bill be limited to the enforcement of serious criminal laws of Australia, with the potential addition of the investigation or prosecution of serious criminal acts or omissions committed overseas where also a serious offence under Australian law. This would allow, if necessary, Australian law enforcement agencies/authorities to access encrypted information to assist overseas agencies in dealing with terrorism, child sex offences, and the other types of conduct which the Bill is designed to address.
- Annual reports should include a percentage breakdown of types of notices issued and whether they were for terrorism, child sex offences, organised criminal activity or otherwise.
- The Law Council notes that many jurisdictions have enacted, or are considering, similar legislation. The Law Council suggests it is important to consider the lack of an invasion of a privacy cause of action in Australia, in contrast to jurisdictions such as the United States. The lack of a privacy cause of action increases the Bill's potential negative impact to personal privacy for which individuals will have little recourse.
- When assistance has been provided under a TAR/TAN/TCN, subjects of an interception warrant or a TAR be notified of the fact once there is no prejudice to an investigation.[8]
- The Law Council's previous recommendation that the Office of the Australian Information Commissioner (**OAIC**) has direct oversight to ensure the Australian Privacy Principles under the *Privacy Act 1988* (Cth) (**Privacy Act**) are complied with be adopted.[9]
- If 'assistance to foreign law enforcement' is to remain as a basis for giving a TAR/TAN/TCN, the Law Council recommends that the relevant decision-maker must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under section 8 of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) (**MACMA**). This must be considered prior to a TAR/TAN/TCN being given, and where the relevant purpose relates to 'assisting the enforcement of the criminal laws in force in a foreign country'.
- The Law Council suggests further that proposed paragraph 317L(2)(d) of the Bill for TANs and proposed subparagraphs 317T(2)(a)(ii) and 317T(2)(b)(ii) for TCNs be removed to balance the protection of the fundamental human right to privacy with the proportionate purposes by which the powers under the Bill are exercised.
- Given that the power to issue a TAN and TCN is significantly intrusive, and likely to require much more active assistance of the recipient, than compliance with a requirement to protected access to content of an unprotected

[8] See similar recommendation in the Joint Select Committee on Cyber-Safety, Parliament of Australia, *Report on the Review of the Cybercrime Legislation Amendment Bill 2011* (2011), 45-57.
[9] Law Council of Australia, 'Policy Statement: Rule of Law Principles' (March 2011), 4.

communication, issuance of a TAN or TCN should require authorisation by a judicial officer (judge or full-time member of the Administrative Appeals Tribunal (**AAT**)).

Additional recommendations

18. In this submission, the Law Council makes the following additional recommendations:

- The Bill should be amended to insert a provision requiring review of the proposed industry assistance framework and computer access warrants scheme by the PJCIS that commences on or before the second anniversary at the end of the implementation phase, and must be concluded on or before the third anniversary at the end of the implementation phase.
- Additional resources for oversight of the activities under Schedule 1 should be made available to the relevant oversight bodies.
- Proposed section 317ZG (a designated services provider must not be required to implement or build a systemic weakness or systemic vulnerability) be amended:
    - to prohibit a TCN or TAN from requiring any act or omission that might require a designated communications provider to either implement or build any weakness or vulnerability into a current or proposed product or service; and
    - to clarify the meaning of a 'systemic weakness' or 'systemic vulnerability**'**.
- There should also be a prohibition on introducing a systemic weakness or vulnerability in relation to TARs.
- Proposed subsection 317T(5) (that the Minister may determine a listed act or thing via legislative instrument) not proceed. Any addition to an act or thing required under a TCN should be by way of legislative amendment.
- In the alternative, the Law Council recommends that proposed subsection 317T(6) (considerations of the Minister) be amended so that considerations required by the Minister in making a determination explicitly include the potential impact on human rights, such as the right to privacy.
- The listed acts or things under proposed section 317E remain exhaustive for TARs and TANs, by removing the words '(but not limited to)' under proposed subsections 317G(6) and 317L(3).
- Proposed sections 317TA, 317MA and 317HA (duration of a TAN, TCN or TAR) of the Bill be amended:
    - to include a maximum time-limit after which a new TAN, TCN or TAR would have to be issued;
    - to include a limit to the number of fresh notices or requests that can be issued.
- The Bill be amended to include a periodic review stage of a TAN, TCN or TAR to assist oversight and accountability agencies.
- Proposed paragraphs 317RA(c) and 317ZAA(c) (considerations regarding whether requirements imposed by a TAN or TCN are reasonable and proportionate) be amended to read 'the legitimate interests of the designated communications provider to whom the notice relates, including commercial interests'.
- The Bill be amended to remove proposed paragraphs 317RA(g) and 317ZAA(g) – such other matters (if any) as the Attorney-General, Director-General of the Security or the chief officer, as the case requires, considers relevant.

- Proposed paragraphs 317RA(f) and 317ZAA(f) (the legitimate expectations of the Australian community relating to privacy and cybersecurity) should be amended to refer explicitly to the fundamental human right to privacy. In the alternative, proposed paragraphs 317RA(f) and 317ZAA(f) should 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.
- Further factors should be listed which require the issuer of a TAN or TCN to separately consider the potential legal consequences to the recipients of warrants.
- The Law Council considers that there should also be a requirement for necessity and proportionality in the decision-making criteria for the issuance of a TAR.
- Proposed sections 317G and 317ZJ which confer civil immunity on providers issued with a TAR, TAN or TCN, be amended:
    - to include limitations on the conferral of civil liability for providers who comply with a TAR, TAN or TCN so that civil immunity is not conferred if the conduct results in significant loss of, or damage to, property, economic loss or physical or mental harm or injury (in line with proposed section 21A of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**);
    - to include limitations and exceptions, to the extent possible that reflect those available in the controlled operations scheme and appropriately modified as required for intelligence agencies.
- In relation to the Australian Security Intelligence Organisation (**ASIO**), the conferral of immunity powers in relation to TARS under proposed subsection 317G(1) of the Telecommunications Act should be by the Attorney-General.
- Proposed subsection 476.2(4) of the *Criminal Code Act 1995* (Cth) (**Criminal Code**), which confer criminal immunity, be further amended to explicitly state that a TAN or TCN given no legal effect under proposed sections 317ZG and 317ZH will not confer criminal immunity.
- The application of criminal immunity under proposed subparagraph 476.2(4)(b)(iv) of the Criminal Code for TARs be limited, so that criminal immunity is only conferred in relation to acts done in accordance with a TAR.
- Consideration be given to civil indemnification rather than immunity for providers.
- Where the ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.
- The Bill should be amended to require annual reporting to the Parliament on the number of times the immunities are used; the kinds of assistance requested and provided; and the extent to which the immunity provisions did not apply.
- The 'reasonable and proportionate' test should specifically require the decision maker to determine whether use of the measure is necessary in the investigation or enforcement of laws in relation to investigation or enforcement of a serious offence in circumstances where imperatives of law enforcement demonstrably outweigh reasonable expectations of confidentiality in communications of affected individuals and businesses.
- The legislation should clearly identify the intended graduated operation of TAR, TAN and TCN powers.
- Proposed subsection 317ZFA(1) be amended so that a court may make an order they consider appropriate in relation to the disclosure, protection, storage, handling or destruction, the proceeding of, TAN, TCN or TAR information, if the court is satisfied that it is in the interests of justice to make such orders.

- The Bill be amended so that decisions made under Schedule 1 are made by a judicial officer and not the Attorney-General.
- In the alternative, the Law Council recommends that judicial review of Schedule 1 decisions under the *Administrative Decisions (Judicial Review) Act* (Cth) (**ADJR Act**) should be available.
- The secrecy offence in proposed subsection 317F(1) should be amended to include an express harm requirement.
- The proposed secrecy offence should be amended to include a more comprehensive list of defences as applies with other secrecy provisions such as those in the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth).
- Proposed paragraph 27E(2)(b) of the *Surveillance Devices Act 2004* (Cth) (**Surveillance Devices Act**), which authorises a computer access warrant to enter any premises for the purposes of gaining entry to, or exiting, the specified premises, be amended so that access to third party premises, computer or communication in transit should be limited to cases where an eligible Judge or nominated AAT member considers it is necessary (rather than appropriate) in the circumstances to execute the warrant, having regard to the human rights of the relevant parties including their right to privacy. Paragraphs 25A(4)(aaa) and 25A(8)(e) of the ASIO Act, proposed subparagraph 3F(2A)(c)(i), proposed subparagraph 3F(2D)(b) and proposed section 3F(2E) of the *Crimes Act 1914* (Cth) (**Crimes Act**), and proposed subparagraphs 199(4A)(c)(i) and 199B(2)(c)(i), and proposed paragraphs 199(4C)(b) and 199B(4)(b) of the *Customs Act 1901* (Cth) (**Customs Act**) should be subsequently be amended.
- While the Law Council recognising the different features of telecommunication intercept warrants and computer access warrants, are different, in the absence of evidence to suggest why amendments to existing thresholds in relation to telecommunications interception should be lowered, the Bill should be amended to retain the existing thresholds that apply for the purposes of the new computer access warrants in the ASIO Act and SDA. This requires for example that:
    - existing thresholds for ASIO a computer access warrant, foreign intelligence warrant or identified persons warrant allowing the interception of a communication passing over a telecommunications system can only be authorised by the Attorney-General if the Attorney-General is satisfied that the telecommunications service is being or is likely to be used for purposes prejudicial to security;
    - telecommunications interception under a computer access warrant should be limited to relevant offences under the SDA that are serious offences under the TIA Act; and
    - the Judge or nominated AAT member must not issue a warrant under the SDA where a control order is in force in relation to another person, and the particular person is likely to communicate with the other person using the service unless he or she is satisfied that the agency has exhausted all other practicable methods or interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.
- In the absence of such justification, and if the telecommunications interception power in the new computer access warrants is to proceed, it should be limited to the purpose of obtaining access to 'relevant data' as defined for example under

existing paragraphs 25A(4)(a) and 27E(2)(c) and (d) of the ASIO Act and proposed paragraphs 25A(4)(ab) of the ASIO Act and 27E(2)(c) of the SDA.

- In the absence of such justification, the authorisation of the use of force should be prohibited for the telecommunications interception power in the new computer access warrants.
- Reporting requirements for the significantly expanded computer access warrants regime should include a requirement to report on the details of the telecommunications service to or from which *each intercepted communication* was made.
- 'General computer access intercept information' should be subject to the use, storage and destruction requirements in the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) and the SDA, rather than excluded from their operation.
- The Bill should be amended to outline that telecommunications intercepts will not be permitted under emergency authorisations as is consistent with existing subsection 32(4) of the SDA.
- In the absence of such justification, and if the temporary removal power in the new computer access warrants is to proceed, it should be limited to the purpose of obtaining access to 'relevant data' under existing paragraphs 25A(4)(a) and 27E(2)(c) and (d) of the ASIO Act and proposed paragraphs 25A(4)(ab) of the ASIO Act and 27E(2)(c) of the SDA.
- The criteria for what objects may be temporarily removed should be clearly set out in the legislation to ensure that there is a rational connection with the legitimate objective of the legislation.
- A maximum time limit should be placed on the period of removal.
- There should be a requirement to aid transparency to report on all temporary removals under computer access warrants.
- The term 'or otherwise' in proposed paragraph 27D(1)(b)(ix) should be more clearly defined. Proposed paragraph 27D(1)(b)(ix) provides that a computer access warrant must specify, if the target computer is or includes a computer associated with, used by or likely to be used by, a person – the person (whether by name or otherwise).
- Proposed paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) of the ASIO Act and proposed paragraphs 27E(7)(k) of the SDA, which relate to the duration of concealment activities, should not proceed. In the alternative, 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.
- Proposed section 64AD of the SDA (compulsory assistance to law enforcement relating to data) and section 34AAA of the ASIO Act (compulsory assistance to ASIO) should clearly outline whether the 'specified person' is a natural person or a legal person.
- The PJCIS consider reducing the penalty available under proposed sections 64A and 34AAA of the Bill to be proportionate to the penalties relating to a 'serious offence' under the Crimes Act.
- Proposed sections 34AAA of the ASIO Act and 64A of the SDA, which have the potential for assistance orders to impinge on the privilege against self-incrimination, should be amended to include a 'use' immunity and a 'derivative use' immunity.
- Section 64 of the SDA should be amended ensure liability by the Commonwealth to pay compensation for loss or injury resulting from the unlawful use of a computer access warrant.

- An independent review of the MACMA should be conducted to ensure that Australia is complying with fundamental rule of law principles and its international obligations.
- Consideration should be given to amending the MACMA to clearly define 'special circumstances' for the purposes of mutual assistance in cases where an offence in a foreign country may be punishable by the death penalty.
- In the absence of evidence, the conferral of civil immunity powers for voluntary assistance to ASIO should be by the Attorney-General rather than through internal ASIO authorisation.
- Where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.
- Clarification should be provided as to the intended relationship between the immunity provisions in the case of ASIO.
- In the case of ASIO, the Bill should be amended to ensure that the immunity of civil liability does not cover conduct that causes economic loss or physical or mental harm or injury which might otherwise constitute negligence. Alternatively, it must be clear on the face of the legislation that an aggrieved person would have a legally enforceable remedy against ASIO.
- In the case of ASIO, the procedural framework surrounding voluntary assistance requests made under proposed subsection 21A(1) and the associated immunity from civil liability should be improved to aid transparency and accountability by making it clear:
    - that compliance with a request is voluntary (as proposed for subsection 317HAA(1) of the Telecommunications Act);
    - how long the request will be in force with a maximum statutory period applying;
    - that a voluntary assistance provided to ASIO request does not cover ongoing requirements for assistance;
    - that oral requests should be followed by a written record to the person as soon as reasonably practicable;
    - the manner in which such requests may be varied or revoked; and
    - the manner in which there are reporting requirements under the provisions. The Law Council considers that there should be annual reporting to the Parliament on the number of times the provision is used; the kinds of assistance requested and provided; and the extent to which the civil immunity provision did not apply.
- Proposed subparagraph 34AAA(2)(c)(i) of the ASIO Act should require that a person is knowingly and intentionally involved in activities that are prejudicial to security.
- Schedule 5 of the Bill should make the link between the person being subject of the assistance order and the security matter explicit.
- The Explanatory Memorandum to the Bill should explain why only computers and storage devices not on the premises are subject to proposed subsection 34AAA(3) of the ASIO Act.
- Proposed section 34AAA of the ASIO Act should include adequate record keeping requirements, reporting requirements, instructions for the cessation of

activities and destruction of materials at least consistent with other parts of the ASIO Act.

- The new provisions should have similar reporting requirements integrated into section 34 of the ASIO Act.
- A person should be notified directly that an order exists with information including a specified time period.
- The possibility for detention should be reconsidered. If the possibility for detention is to remain, the Bill should be amended to as a minimum:
    - allow the person to contact a lawyer or family member, where in the former case client confidentiality is preserved;
    - prescribe a maximum period for the giving of assistance;
    - require officers to explain the nature of the order, complaint mechanisms of the Inspector-General of Intelligence and Security (**IGIS**)/Commonwealth Ombudsman or how to challenge the order in a court;
    - require an interpreter if necessary;
    - require that the person is treated humanely and with respect for their human dignity; and
    - require, at the very least, for the person to be brought before a Federal Court Judge for a hearing in camera after 4 hours have elapsed to enable an application for release or extension of time period as per for example existing provisions for the arrest and interview of suspects under the Crimes Act.
- There should be requirements to guard against oppressive use of multiple coercive powers to obtain particular information.
- The Bill should not be enacted until any human rights issues identified by the Parliamentary Joint Committee on Human Rights have been addressed.

Statutory review

19. The Law Council notes that there is no proposed provision under the Bill for statutory review of the operation of the new industry assistance framework and computer access warrants scheme.

20. The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2018 included a provision requiring review of the new data retention scheme by the PJCIS that commenced on or before the second anniversary at the end of the implementation phase, and must be concluded on or before the third anniversary of the end of the implementation phase.[10] The Law Council considers that, given the significance of the measures contained in the Bill, requiring a statutory review of the proposed industry assistance framework and computer access warrants scheme is an important public accountability and transparency measure.

[10] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187N.

Recommendation

- **The Bill should be amended to insert a provision requiring review of the proposed industry assistance framework and computer access warrants scheme by the PJCIS that commences on or before the second anniversary at the end of the implementation phase, and must be concluded on or before the third anniversary at the end of the implementation phase.**

Schedule 1 – Industry assistance

21. Schedule 1 to the Bill proposes to insert a new Part into the Telecommunications Act. This new part, Part 15, would create a scheme for 'designated communications providers' who:

    (a) may be requested to provide assistance under TARs; or

    (b) be compelled under TANs or TCNs;

    to provide various forms of assistance to security and law enforcement agencies. The assistance provided has to be in connection with the 'eligible activities' of those providers.

22. Providers will be immune from civil and criminal liability for the telecommunications and computer offences in meeting the requests and notices from security and law enforcement agencies.

23. Oversight of these schemes will be critical and should be appropriately resourced. It is an additional oversight task to be completed and therefore should attract additional resources for oversight.

Recommendation

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

'Listed acts or things'

24. Proposed section 317E of the Bill provides a list of 'acts or things' that a designated communications provider may be required to do under a TAR,[11] TAN[12] or TCN.[13] These 'acts or things' can require a designated communications provider to undertake an extremely broad range of activities going beyond simply accessing encrypted data, including: installing, maintaining, testing or using software or equipment;[14] assisting with the testing, modification, development or maintenance of a technology or capability;[15] and modifying, or facilitating the modification of, any of

[11] Ibid s 317G(6).
[12] Ibid s 317L(3).
[13] Ibid s 317T(7).
[14] Ibid s 317E(c).
[15] Ibid s 317E(f).

the characteristics of a service provided by the designated communications provider.[16]

25. Although TCNs cannot require a provider to build a new decryption capability under proposed section 317ZG, the safeguard is limited. 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 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.

26. The Law Council recommends that this broad scope of 'listed acts or things' be limited by amending proposed section 317ZG of the Bill to prohibit a TCN or TAN from requiring any act or omission that might require a designated communications provider to either implement or build any weakness or vulnerability into a *current or proposed product or service* rather than into a form of electronic protection.

27. The Law Council notes that proposed section 317ZG would prohibit a TAN or TCN from requiring a provider to introduce a systemic weakness or vulnerability into a form of electronic protection. However, there is no such protection for TARs which may mean intelligence and law enforcement agencies may ask providers to voluntarily introduce a systemic weakness. Further there appears to be ambiguity in what may constitute a 'systemic weakness/vulnerability'. Given the potential security risks involved with the introduction of a systemic weakness, the Law Council considers that there should also be a prohibition on introducing a systemic weakness or vulnerability in relation to TARs.

28. Proposed section 317ZG of the Telecommunications Act should be amended to clarify the meaning of a 'systemic weakness' or 'systemic vulnerability'.

Recommendations

- **Proposed section 317ZG be amended:**
  - **to prohibit a TCN or TAN from requiring any act or omission that might require a designated communications provider to either implement or build any weakness or vulnerability into a current or proposed product or service; and**
  - **to clarify the meaning of a 'systemic weakness' or 'systemic vulnerability'.**
- **There should also be a prohibition on introducing a systemic weakness or vulnerability in relation to TARs.**

Determination of listed acts or things for TCNs by legislation instrument

29. The Law Council notes that under proposed subsection 317T(5), in relation to TCNs, the Minister may, by legislative instrument, determine one or more kinds of acts or

[16] Ibid s 317E(h).

things, in addition to the listed acts or things under proposed section 317E.[17] In making a determination, the Minister must have regard to the interests of law enforcement, the interests of national security, the objects of the Act, the likely impact on the determination on designated communications providers, and such other matters (if any) as the Minister considers relevant.[18]

30. The Law Council is 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, including an assessment of whether the addition to the listed acts of things via legislative instrument is necessary and proportionate. The Law Council recommends that any addition to an act or thing required under a TCN should be by way of legislative amendment, to ensure proper parliamentary oversight, which includes consideration of the necessity and proportionality of the addition to the listed act or thing, including the potential impact on human rights.

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

Recommendations

- **Proposed subsection 317T(5) not proceed. Any addition to an act or thing required under a TCN should be by way of legislative amendment.**
- **In the alternative, the Law Council recommends that proposed subsection 317T(6) be amended so that considerations required by the Minister in making a determination explicitly include the potential impact on human rights, such as the right to privacy.**

Non-exhaustive list of acts or things for TARs and TANs

32. Proposed subsections 317G(6) and 317L(3) provide that an act or thing stated in a TAR or TAN includes, but is not limited to, listed acts or things under proposed section 317E.[19] This means that the listed acts or things that can be required under a TAR or TAN are non-exhaustive.

33. The Law Council understands that a non-exhaustive list may be important to allow the list of acts or things to respond to changes in technology. However, the Law Council is concerned that a non-exhaustive list may allow for the addition of 'listed acts or things' that are not demonstrated to be necessary or proportionate, and may potentially impact on human rights considerations.

34. The Law Council recommends that the listed acts or things under proposed section 317E remain exhaustive for TARs and TANs, by removing the words '(but not limited to)' under proposed subsections 317G(6) and 317L(3).

[17] Other than an act or thing covered by paragraph 317E(1)(a) – removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider (s 317(4)(c)(i)).
[18] *Telecommunications (Interception and Access) Act 1979* (Cth) s 317T(6).
[19] There is a similar proposed subsection for varied TARs under proposed subsection 317JA(10), and for varied TANs under proposed subsection 317Q(9).

Recommendation

- **The listed acts or things under proposed section 317E remain exhaustive for TARs and TANs, by removing the words '(but not limited to)' under proposed subsections 317G(6) and 317L(3).**

Duration of TARs, TANs and TCNs

35. Proposed section 317TA sets out the duration of a TCN. Unless revoked sooner, a TCN remains in force until the end of the expiry date specified in the notice, or if no expiry date is provided, at the end of the 180-day period beginning when the notice was given.

36. Proposed sections 317MA and 317HA set out the duration of TANs and TARs. Unless revoked sooner, a TAN or TAR remains in force until the end of the expiry date specified in the notice or request, or if no expiry date is provided, at the end of the 90-day period beginning when the notice or request was given.

37. Proposed subsections 317TA(2), 317MA(2) and 317HA(2) provide that if a TCN, TAN or TAR expires, a fresh TCN, TAN or TCN in the same terms may still be issued.

38. The Law Council notes that there is no time limit for TARs, TANs and TCNs under proposed sections 317TA, 317MA and 317HA. Under these proposed sections an agency may specify an expiry date for a TAN, TCN or TAR, however there is no limit provided in the Bill for a maximum amount of time a request or notice is to remain in force. A period of years could therefore be specified by the agency making the request or issuing the notice. A fresh TAN, TCN or TAR in the same terms can be issued after an expiry date, however there is no limit to the number of fresh notices or requests that can be issued.

39. Given such potential long-term impositions on individuals or companies, a request or notice could have significant resourcing implications for a designated services provider issued with a TAR, TAN or TCN. Proposed subsection 317ZK(3) provides for a no profit, no loss model for a designated services provider complying with a notice or request, however the actual cost recovery is not guaranteed, and over the long term may become problematic. Given that some notices may be compulsory, the long-term duration and lack of a guaranteed resource recovery may prove to be problematic for some designated communications providers.

40. The Bill does not appear to include a periodic review provision to have requests and notices reviewed after a certain period. Such a review stage would give providers an opportunity to raise concerns regarding the requirements under a TAR, TCN or TAN. It would also assist oversight and accountability agencies in their compliance work. Given the potentially coercive and onerous demands on providers and intrusive methods for targets, regular oversight and accountability mechanisms should be included.

Recommendations

- **Proposed sections 317TA, 317MA and 317HA of the Bill be amended:**
  - **to include a maximum time-limit after which a new TAN, TCN or TAR would have to be issued; and**
  - **to include a limit to the number of fresh notices or requests that can be issued.**
- **The Bill be amended to include a periodic review stage of a TAN, TCN or TAR to assist oversight and accountability agencies.**

Decision-making criteria – considerations that a TCN or TAN are reasonable and proportionate

41. Proposed sections 317P, 317Q(10), 317V and 317X(4) require that, before issuing or varying a TAN or TCN, the decision-maker must be satisfied that:

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

    (b) compliance with the notice is practicable and technically feasible.

42. The Law Council supports in part proposed sections 317RA and 317ZAA of the Bill which list the matters that must be considered when deciding whether the requirements imposed by a TAN or a TCN are reasonable and proportionate. Proposed sections 317RA and 317ZAA state that when considering whether the requirements imposed by a TAN, a varied TAN, and TCN or a varied TCN are reasonable and proportionate, the Director-General of Security or the chief office of an interception agency (for a TAN) or the Attorney-General (for a TCN), as the case requires, must have regard to:

    (a) the interests of national security;

    (b) the interests of law enforcement;

    (c) the legitimate interests of the designated communications provider to whom the notice relates;

    (d) the objectives of the notice;

    (e) the availability of other means to achieve the objectives of the notice;

    (f) the legitimate expectations of the Australian community relating to privacy and cybersecurity;

    (g) such other matters (if any) as the Director-General of Security or the chief officer, as the case requires, considers relevant.

43. In particular, the Law Council supports proposed paragraphs 317RA(e) and 317ZAA(e) which require the issuer to consider the availability of other means to achieve the objectives of the notice. This is consistent with the Law Council's recommendation to the Department that the Exposure Draft Bill be amended so that the issuer must consider reasonable alternatives as may be available to the grant of the notice.

44. However, the Law Council notes the following concerns regarding the factors to be considered under proposed sections 317RA and 317ZAA.

45. The proposed criteria do not provide guidance on how the individual factors are to be weighed or balanced when considering whether a TCN or TAN is reasonable and proportionate. This may mean in practice that, for example, higher weight is always given to the interests of national security and law enforcement rather than the other factors listed. The threshold of the individual factors are low, for example, 'the interests of national security or law enforcement' may capture a broad range of benign activity. The Law Council recommends that proposed paragraphs 317RA(a)-(b) and 317ZAA(a)-(b) be amended to include a higher threshold of significant or serious national security and law enforcement interests.

46. The Law Council considers that while proposed paragraphs 317RA(c) and 317ZAA(c) – 'legitimate interests of the designated communications provider to whom the notice relates' – may require the issuer of a TAN or TCN to consider the likely cost of complying with a notice, this should be explicitly listed as a consideration under sections 317RA and 317ZAA in order to avoid confusion. It may be appropriate for costs of compliance to be an additional matter for consideration by the issuer with respect to TANs or TCNs where the mandatory aspect of the notices means that Australian intelligence services may compel designated service providers to undertake extensive and potentially resource-draining activities in response to assistance requests from foreign law enforcement agencies. The Law Council recommends that proposed paragraphs 317RA(c) and 317ZAA(c) be amended to read 'the legitimate interests of the designated communications provider to whom the notice relates, including commercial interests'.

47. The Law Council is concerned that proposed paragraphs 317RA(g) and 317ZAA(g) – 'such other matters as the Director-General of Security or the chief officer, as the case requires, considers relevant' – may operate as a basic catch-all provision with a low threshold that allows the issuer to consider a broad range of factors when deciding to issue a TCN or TAN. The Law Council recommends that the Bill be amended to remove proposed paragraphs 317RA(g) and 317ZAA(g). Further, the Law Council recommends that proposed sections 317RA and 317AA are amended to make clear that the matters listed are exhaustive, by inserting 'or' or 'and' after each matter listed.

48. Proposed paragraphs 317RA(f) and 317ZAA(f) – 'the legitimate expectations of the Australian community relating to privacy and cybersecurity' – may be overly broad and vague. Proposed paragraph (f) should be amended to refer explicitly to the fundamental human right to privacy. In the alternative, proposed paragraph (f) should 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.

49. The Law Council recommends that further factors should be listed which require the issuer of a TAN or TCN to separately consider the potential legal consequences to the recipients of warrants.

50. The Law Council also notes that the decision-making criteria before the issuance of a TAR are far more limited to where the decision-maker request a designated communications provider to do acts or things,[20] which must be in the exercise of a

[20] Telecommunications and Other Legislation Amendment (Interception and Access) Bill 2018 sch 1 item 7, s 317G(1)(a)(v-vi).

function or power of the requesting agency and in relation to a relevant objective.[21] A relevant objective for the purposes of this section are outlined in paragraphs 317(5)(a)-(c) as meaning:

(a) enforcing the criminal law and laws imposing pecuniary penalties; or

(b) assisting the enforcement of the criminal laws in force in a foreign country; or

(c) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

51. The Law Council considers that there should also be a requirement for necessity and proportionality in the decision-making criteria for the issuance of a TAR.

Recommendations

- **Proposed paragraphs 317RA(c) and 317ZAA(c) be amended to read 'the legitimate interests of the designated communications provider to whom the notice relates, including commercial interests'.**
- **The Bill be amended to remove proposed paragraphs 317RA(g) and 317ZAA(g) – such other matters (if any) as the Attorney-General, Director-General of the Security or the chief officer, as the case requires, considers relevant.**
- **Proposed paragraphs 317RA(f) and 317ZAA(f) should be amended to refer explicitly to the fundamental human right to privacy. In the alternative, proposed paragraphs 317RA(f) and 317ZAA(f) should refer to the Australian Privacy Principles under the *Privacy Act 1988* (Cth), and the potential privacy impact of a TAN or TCN be evidenced by a privacy impact assessment undertaken by the OAIC.**
- **Further factors should be listed which require the issuer of a TAN or TCN to separately consider the potential legal consequences to the recipients of warrants.**
- **The Law Council considers that there should also be a requirement for necessity and proportionality in the decision-making criteria for the issuance of a TAR.**

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

52. Under proposed paragraph 317G(1)(c) a provider who complies with a TAR, or acts in good faith purportedly in accordance with a TAR, and provides assistance to ASIO, ASIS, ASD or an interception agency, is immune from civil liability. Similarly, under proposed subsection 317ZJ(1), a provider who complies with a TAN or TCN, or acts in good faith in purported compliance, is immune from civil liability.

53. Proposed sections 317G(1)(d) and 317ZJ(3) state that civil immunity extends to all employees, officer and agents of a relevant provider, meaning that a potentially broad range of people who comply with a TAR, TAN or TCN are protected from civil immunity.

[21] Ibid s 317G(2)(a)(v).

54. The Law Council notes the special intelligence operations (**SIO**) of the ASIO Act under section 35K which contains a number of exceptions and limitations to the conferral of liability during SIOs. The SIO scheme contains a number of further limitations on SIOs that enhance oversight of the scheme, such as reporting and notification requirements to IGIS and the Attorney-General,[22] the requirement that an SIO can only be granted by the Attorney-General,[23] and a number of requirements the Attorney-General must consider when granting a SIO such as any unlawful conduct involved in conducting the SIO will be limited to the maximum extent consistent with conducting an effective SIO.[24]

55. The *Intelligence Services Act 2001* (Cth) (**ISA**) provides limitations on the conferral of civil and criminal immunity to staff or agents of ASD, AGO or ASIS. Civil and criminal immunity is only available if an act is preparatory to, in support of or otherwise directly connected with, overseas activities of the agency and the act is done in proper performance of a function of the agency.[25] The same limitations are applied on civil and criminal immunities relating to any computer-related act under the Criminal Code.[26]

56. The Australian Federal Police's (**AFP**) controlled operations scheme also contains a number of important safeguards on the conferral of criminal immunity and civil indemnification:[27]

    (a) it is limited for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious offence;[28]

    (b) it limits the proposed protections from civil and criminal liability provided under the controlled operations scheme so that civil indemnification, rather than immunity, is provided to participants;[29]

    (c) compensation in respect of serious property damage or personal injury is required;[30]

    (d) participants would only be immune or indemnified from liability if their conduct was *likely* to cause death, serious injury or result in the commission of a sexual offence;[31]

    (e) civilians would need to act in accordance with the instructions of a law enforcement officer; [32] and

    (f) detailed reporting to the Commonwealth Ombudsman and the relevant Minister, clear record-keeping obligations and obligations on the

[22] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 35PA and 35Q.
[23] Ibid s 35B-35C.
[24] Ibid s 25C(2)(c).
[25] *Intelligence Services Act 2001* (Cth) s 14(2).
[26] *Criminal Code Act 1994* s 476.5(2).
[27] The Law Council has noted that these safeguards do not apply to the SIO scheme, and have previously recommended the SIO scheme be amended to align with the controlled operations scheme. See Law Council of Australia, Submission No 75 to the Australian Law Reform Commission, *Traditional Rights and Freedoms – Encroachment by Commonwealth Laws* (March 2015), 44-45.
[28] *Crimes Act 1914* (Cth) ss 15GD(1)(b) and 15GE.
[29] Ibid s 15HB.
[30] Ibid s 15HF.
[31] Ibid s 15HA(2)(d).
[32] Ibid ss 15HA (2)(e) and 15HB(f).

Commonwealth Ombudsman to regularly inspect and report to the Minister is included.[33]

57. The Law Council further notes that the limitations on civil liability immunity under proposed section 21A(1) of the ASIO Act, for persons who provide voluntary assistance to ASIO, contain important limitations on the immunity. Under proposed subsection 21A(1) a person or body who complies with a voluntary assistance request does not receive civil immunity if the conduct results in significant loss of, or serious damage to, property.[34]

58. In its submissions to the Australian Law Reform Commission (**ALRC**) regarding its 2014 inquiry into *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws,* the Law Council previously noted that the rule of law requires that the Executive Government be responsible in law to the same extent and in the same way as an ordinary citizen, including when the Government contracts or commits an intentional act or omission.[35] Executive immunity from civil action has generally been in decline in Australia.[36]

59. The Law Council is concerned that the proposed sections conferring civil immunity from providers who comply with a TAR, TAN or TCN are overly broad, and do not contain important safeguards on the operation of the conferral, such as exclusions or express limitations on the operation of the civil immunity. This means that third parties who have their rights breached, including significant loss of, or serious damage to, property, economic loss or physical or mental harm or injury, not be able to recover damages or obtain other legal remedies.

60. The Law Council considers that similar safeguards should be made available regarding the conferral of civil immunity from the proposed industry assistance scheme under proposed Part 15 of the Bill.

Recommendations

- **Proposed sections 317G and 317ZJ be amended:**
  - **to include limitations on the conferral of civil liability for providers who comply with a TAR, TAN or TCN so that civil immunity is not conferred if the conduct results in significant loss of, or damage to, property, economic loss or physical or mental harm or injury (in line with proposed section 21A of the ASIO Act); and**
  - **to include limitations and exceptions, to the extent possible that reflect those available in the controlled operations scheme and appropriately modified as required for intelligence agencies.**

Internal authorisation for the conferral of civil immunity in relation to TARs

61. Proposed subsection 317G of the Telecommunications Act confers an immunity from civil liability on a designated services provider who renders voluntary technical

[33] Ibid Division 4.
[34] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 5 item 2, s 21A(1)(e).
[35] Law Council of Australia, Submission No 140 to the Australian Law Reform Commission, *Interim Report on Traditional Rights and Freedoms – Encroachment by Commonwealth Laws* (9 October 2015), 48.
[36] Ibid.

assistance under a TAR in accordance with a request by the Director-General of Security, ASIS or the ASD, or the chief officer of an interception agency. Under proposed section 317ZM interception agency includes law enforcement agencies such as the AFP. This proposed internal authorisation would represent a significant expansion of power as currently only the Attorney-General may confer a civil immunity on participants in a SIO.

62. Proposed subsection 317G(1) of the Telecommunications Act provides that if the Director-General or chief officer of an interception agency requests a designated communications provider to do one or more specified act that is in connection with any or all of the eligible activities of the provider, and the provider acts in accordance with the request or in good faith purportedly in accordance with the request, then the provider, or any officer, employee or agent of the provider, is not subject to any civil liability.

63. The Law Council does not consider that the internal authorisation for the conferral of civil immunity has been demonstrated to be necessary and proportionate. In the absence of such evidence, the conferral of civil immunity powers should be by the Attorney-General (in the case of ASIO).

Recommendation

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

Conferral of criminal immunity on providers issued with a TAR, TAN or TCN

64. Proposed subparagraphs 476.2(4)(b)(iv)-(vi) of the Bill would amend the Criminal Code to allow a person who causes any access, modification or impairment of a computer, data held on a computer, an electronic communication to or from a computer, or in relation to the reliability, security or operation of data held on an electronic data storage device, to do that act if done in accordance with the a TAR, or in compliance with a TAN or TCN, that causes any access. In other words, this means that a person that causes access, modification or impairment, will not be criminally liable of an offence if they do so under a TAR, TAN or TCN.

65. The Law Council understands the need to confer criminal liability on providers who comply with a TAR, TAN or TCN, in order to compel providers to provide assistance under the request or notice. However, the Law Council considers that the conferring of criminal immunity under the Bill is currently too broad and should be limited in a manner similar to subparagraph 476.2(4)(b)(i) of the Criminal Code which provides that a criminal immunity can only be conferred if a person does not exceed the limits of their authority under a warrant.

Potential conferral of criminal immunity on legally ineffective TANs or TCNs

66. The Law Council notes the limitations placed on TCNs and TANs under proposed sections 317ZG and 317ZH of the Bill. A TAN or TCN has no effect to the extent (if any) to which it would require a provider to implement or build a systemic weakness,

or a systemic vulnerability, into a form of electronic protection,[37] or prevents a provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.[38] A TAN or TCN also does not have any effect to the extent (if any) to which it would require a provider to do an act or thing for which a warrant or authorisation is required.[39]

67. However, proposed paragraph 476.2(4)(b)(v)-(vi) of the Bill, which amends the Criminal Code, does not explicitly provide that a TAN or TCN which has no legal effect under proposed sections 317ZG and 317ZH will not be conferred criminal immunity. There may be a legal argument that a TAN or TCN with no legal effect under proposed sections 317ZG and 317ZH does not constitute a 'notice' under proposed paragraph 476.2(4)(b)(v)-(vi) of the Criminal Code.

Recommendation

- **Proposed subsection 476.2(4) of the Criminal Code be further amended to explicitly state that a TAN or TCN given no legal effect under proposed sections 317ZG and 317ZH will not be conferred criminal immunity.**

Appropriateness of civil and criminal immunity in relation to a TAR

68. The Law Council understands that some level of immunity should apply regarding TANs and TCNs due to their compulsory nature. However, the Law Council queries whether a TAR, which requires a provider to voluntarily provide assistance, should be provided with the broad immunities under proposed subparagraph 476.2(4)(b)(iv) of the Criminal Code (criminal immunity) and under proposed paragraph 317G(1)(c) of the Telecommunications Act (civil immunity).

69. As noted, the Law Council considers that there should be a requirement for necessity and proportionality in the decision-making criteria for the issuance of a TAR.

70. In relation to the conferral of criminal immunities and TARs, the Law Council notes that there does not appear to be a requirement that criminal immunity is only conferred in relation to acts done in accordance with a TAR. This requires clarification.

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

72. In relation to the conferral of civil immunities for TARs, the Law Council recommends that consideration be given to civil indemnification rather than immunity for providers. Where an immunity would protect a provider from all forms of civil liability by removing the right of any party to commence action for loss or damage caused by the provider, civil indemnification is more limited. For example, civil

[37] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 1 item 7, s 317ZG(1)(a).
[38] Ibid s 317ZG(1)(b).
[39] Ibid s 317ZH(1)-(3).

indemnification may be limited to financial liability or indemnity in relation to certain specified conditions.

Recommendations

- **The application of criminal immunity under proposed subparagraph 476.2(4)(b)(iv) of the Criminal Code for TARs be limited, so that criminal immunity is only conferred in relation to acts done in accordance with a TAR.**
- **Consideration be given to civil indemnification rather than immunity for providers.**
- **Where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.**

Reporting requirements for conferral of immunities

73. The Law Council considers that the Bill should be amended to require annual reporting to the Parliament on the number of times the immunities are used; the kinds of assistance requested and provided; and the extent to which the immunity provisions did not apply. There should also be reporting on the instances where a provider engaged in conduct in accordance with a TAR, TAN or TCN causes significant loss of, or serious damage to, property, or significant financial loss, or where the provider engaged in conduct in purported compliance with a TAR, TAN or TCN and is excluded from the immunity.

74. The Law Council considers this would improve oversight and accountability regarding the conferral of civil and criminal immunity for acts done in accordance with a TAR, TAN and TCN.

Recommendation

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

Requirement to consider the investigation or enforcement of laws ancillary to a serious offence

75. As noted above, the Law Council has previously recommended the Bill be limited to the enforcement of serious criminal laws of Australia, with the potential addition of the investigation or prosecution of serious criminal acts or omissions committed overseas where also a serious offence under Australian law. In addition, the Law Council is concerned that the extension of the measures to include exercise of a law enforcement power in relation to such lesser unlawful acts, also includes a matter 'that facilitates, or in ancillary and incidental to', such lesser unlawful acts. Determination of whether use of the measures is 'reasonable and proportionate' is in respect of a particular investigation of any of a broad range of acts (and ancillary activities) suspected to have occurred within any of a broad range of unlawful acts. That is, the determination is act- and offence-specific, and not within the broader context of the appropriate balancing of societal interests and individual autonomy.

76. The decision-making criteria do not task the relevant decision maker, when making a 'reasonable and proportionate' determination, to determine whether perceived law enforcement imperatives of law enforcement agencies should outweigh affected individuals' and businesses' reasonable expectations of confidentiality in communications. Indeed, the Bill does not specifically acknowledge that individuals and businesses are entitled to any reasonable expectation of confidentiality in communications, and that overriding that expectation may adversely affect digital trust of citizens and businesses in Australia as a reliably secure place to conduct business.

Recommendation

- **The 'reasonable and proportionate' test should specifically 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.**

Accountability and oversight

77. Proposed subsection 317ZH(1) places general limits on TANs and TCNs, by stating that they have no effect to the extent (if any) to which it would require a designated communications provider to do an act or thing for which a warrant or authorisation under any of the following laws is required:

(a) The TIA Act;

(b) The SDA;

(c) The Crimes Act;

(d) The ASIO Act;

(e) The ISA;

(f) The law of the Commonwealth (other than in this Part) that is not covered by paragraph (a), (b), (c), (d) or (e);

(g) A law of a State or Territory.

78. The Law Council supports the addition of paragraphs 317ZH(1)(f)-(g) in the Bill as a catch-all provision. This is consistent with the Law Council's recommendation to the Department that the legislation should expressly state that the power to request or require decryption (or an individual to facilitate opening up a password protected device) under a TAN or TCN does not displace the need for an agency to obtain lawful authority to view the content of a community or electronic record.[40]

[40] Law Council of Australia, Submission to the Department of Home Affairs, *Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* available online https://www.lawcouncil.asn.au/docs/6e0bcb0a-44bd-e811-93fc-005056be13b5/3504%20-%20Assistance%20and%20Access%20Bill%202018.pdf, 7.

79. However, the Law Council maintains its concern submitted to the Department that this limitation is unlikely to be understood by many individuals within the diverse range of agencies that may utilise these powers and the greatly expanded range and nature of recipient entities within and outside Australia that will be subject to complex Australian law enforcement legislation for the first time, and their respective legal advisers. In particular, the Bill purports to apply to providers outside Australia of an electronic service that has one or more end-users in Australia (proposed sections 317C and 317D), and the encrypted communication may have no other relevant link to Australia or to that of those end-users in Australia, so the provider may have little or no familiarity with Australian law. In any event, the limitation is fundamental in determining whether the Bill undermines security and confidentiality of a wide range of communications (including financial transactions flowing through the international banking system) or is an unreasonable interference in the fundamental human right to privacy.

Graduated operation of a TAR, TAN and TCN

80. The Law Council supports in part proposed section 317HAA of the Bill, which states that if a TAR is issued to a designated communications provider, the request must advise the provider that compliance with the request is voluntary. Further, proposed sections 317MAA and 317TAA provide that the issuer of a TAN and TCN must give a designated communications provider advice relating to the provider's obligations arising from the request or notice under proposed sections 317ZA or 317ZB.

81. The Law Council supports this amendment to the Exposure Draft Bill as consistent with its recommendation to the Department that the legislation should clearly identify the intended graduated operation of TAR, TAN and TCN powers.

82. However, the Law Council maintains its recommendation to the Department that generally there should be a graduated operation from a TAR, a TAN and a TCN.

83. The Law Council accepts that a law enforcement or national security agency should not be required to proceed in sequential order through the graduated steps of a TAR, a TAN and a TCN in dealings with a particular recipient in relation to a particular form of encryption where prior dealings with the relevant recipient give an agency reasonable grounds to believe that it will be necessary to proceed to a higher step in order to obtain a practically useful response. However, this graduation should be followed except where the requesting agency has reasonable cause to believe, having regard to prior dealings (which may or may not include the requesting agency) with the relevant recipient, that it will be necessary to proceed to a higher step in order to achieve a practically useful response.

Recommendation

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

Consideration of public interest

84. The Law Council notes proposed section 317ZFA which allows a court to make orders as they consider appropriate in relation to the disclosure, protection, storage, handling or destruction, in the proceeding of, TAN, TCN or TAR information, if the court is satisfied that it is in the public interest to make such orders.

85. However, the Law Council recommends that proposed subsection 317ZFA(1) be further amended so that the court is satisfied that it is in the interests of justice, rather than the public interest, to make an order. Under proposed sections 317RA and 317ZAA, in considering whether the requirements imposed by a TCN or TAN are reasonable and proportionate, the issuer must already consider matters relating to the public interest, including the interests of national security and the legitimate expectations of the Australian community relating to privacy and cybersecurity. The Law Council is of the view that consideration of interests of justice by the court is consistent with considerations under the SDA in relation to the regulation and protection of the use of surveillance devices[41] and the ASIO Act in relation to special intelligence operations.[42]

Recommendation

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

Judicial review

86. Item 1 of Schedule 1 of the Bill would insert proposed paragraph (daaa) into Schedule 1 of the ADJR Act with the effect that decisions made under Schedule 1 of the Bill will be excluded from judicial review under the ADJR Act.

87. The Law Council understands in this context why decision-making must be prompt and confidential, but these factors can be addressed with involvement of a judicial officer in the original decision.

88. In New South Wales, for example, the Chief Judge of the district court rosters a judge to deal by telephone with New South Wales Police surveillance warrant requests. The process appears to function effectively and is timely.

89. The Law Council's view is that the best opportunity to ensure that the proposed regime in the Bill is necessary and proportionate is, firstly, to expressly require decision making criteria to have reference to balancing privacy interests (so that reasonableness and necessity are not judged solely by reference to the success or otherwise of a particular investigation); and secondly 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.

90. Ideally, that would be a judicial officer and not the Attorney-General (although the Law Council acknowledges the latter currently provides warrants for security agencies).

91. In the event that our proposal is not accepted, then judicial review of decisions under the ADJR Act should be available. The ADJR Act offers applicants a simplified review process that allows courts to be more flexible in tailoring remedies for the particular circumstances of the case.

[41] *Surveillance Devices Act 2004* (Cth) ss 4 and 47(6).
[42] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35A.

Recommendations

- **The Bill be amended so that decisions made under Schedule 1 are made by a judicial officer and not the Attorney-General.**
- **In the alternative, the Law Council recommends that judicial review of Schedule 1 decisions under the ADJR Act should be available.**

Unauthorised disclosure of information

92. Proposed subsection 317F(1) would create a new secrecy offence for disclosures of information about TARs, TANs and TCNs. This includes disclosing the mere existence of the requests or notices. Under proposed subsection 317ZF(3) there are some exceptions to this secrecy provision such as legal proceedings, the work of the IGIS, disaggregated statistical reporting and information sharing between requesting agencies. Breaching the secrecy provision attracts a penalty of up to five years imprisonment.

93. The Explanatory Memorandum states that:

> *The offence in new subsection 317ZF(1) does not include an express requirement of harm, and therefore, the prosecution is not required to prove harm beyond reasonable doubt …. it is assumed that disclosure is inherently harmful*.[43]

94. In accordance with the ALRC Report *Secrecy Laws and Open Government in Australia* (**Secrecy Report**), the Law Council supports the view that:

> *Specific secrecy offences are only warranted where they are necessary and proportionate to the protection of essential public interests of sufficient importance to justify criminal sanctions.*[44]

95. In the Secrecy Report the ALRC recommended that:

> *Specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest.*[45]

96. The Law Council considers that the secrecy offence in proposed subsection 317F(1) should include an express harm requirement.

97. In addition, if the proposed secrecy provision is to be included, it should include a more comprehensive list of defences such as was created for the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*. Such defences may include communicating information to the Ombudsman, OAIC or the Australian Commission for Law Enforcement Integrity or in accordance with *Public Interest Disclosure Act* (2013) (Cth) or freedom of information requirements.

98. The proposed secrecy offence should be amended to include a more comprehensive list of defences as applies with other secrecy provisions such as

[43] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 65.
[44] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009), Recommendation 8-1.
[45] Ibid Recommendation 8-2.

those in the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth).

Recommendations

- **The secrecy offence in proposed subsection 317F(1) be amended to include an express harm requirement.**
- **The proposed secrecy offence should be amended to include a more comprehensive list of defences as applies with other secrecy provisions such as those in the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth).**

Schedule 2 – Computer access warrants

99. Schedule 2 of the Bill would establish a new computer access warrant regime for law enforcement agencies and significantly enhance ASIO's existing computer access powers.

100. Currently, the ability of ASIO to apply for a computer access warrant falls within ASIO's special powers within Part 3 Division 2 Subdivision C of the ASIO Act. Schedule 2 of the Bill would amend ASIO's computer warrant access powers in sections 25A (computer access warrant), 27A (foreign intelligence) and 27E (identity person warrant) of the ASIO Act. Specifically, key amendments would allow ASIO to:

(a) enable the intercepting of a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing specified in the warrant;[46]

(b) temporarily remove a computer or other thing from premises for the purposes of doing any thing specified in the warrant;[47] and

(c) do things that conceal access to a computer, including for up to 28 days after the warrant ceases to be in force, or as soon as reasonably practicable after the 28-day period.[48]

101. Similar amendments are proposed under the SDA to allow for law enforcement agencies to obtain covert computer access warrants in respect of offence investigations (where an offence against the law of the Commonwealth is punishable by a maximum term of three years imprisonment or more), recovery

[46] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 2 items 6 and 11; Subsection 27A(1) of the ASIO Act would mean that the power in new paragraph 25A(4)(ba) would also be applied to foreign intelligence warrants.
[47] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 2 items 5 and 10; Subsection 27A(1) of the ASIO Act would mean that the power in new paragraph 25A(4)(ac) would also be applied to foreign intelligence warrants.
[48] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 2 items 7, 8 and 12.

orders, mutual assistance investigations, integrity operations and control orders.[49] An application must be made to an eligible judge or to a nominated AAT member.[50]

102. The Bill amends the definition of 'computer' under subsection 6(1) of the SDA, so that the definition would mean one or more computers, computer systems, computer networks, or any combination of the three. The Explanatory Memorandum notes that this amended definition aligns with the definition of 'computer' under the ASIO Act, and that the new broadened definition 'takes into account the increasing use of distributed and cloud-based services for processing and storing data', including mobile phones.[51]

103. Schedule 2 of the Bill also amends the SDA to allow a foreign country requesting access to data held on a computer in relation to a criminal offence in that country, to apply a mutual assistance application, which allows for a computer access warrant via an eligible law enforcement officer.

Privacy impact on third parties

104. The Law Council considers that proposed paragraph 27E(2)(b) of the SDA which authorises a computer access warrant to enter any premises for the purposes of gaining entry to, or exiting, the specified premises, would allow access to third party premises.[52] Similarly, proposed paragraph 27E(2)(e) allows access to an innocent third party's computer or communication in transit to obtain access to relevant data, however with the additional safeguards that the judge or AAT members must consider it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data which are likely to be as effective. These are consistent with existing section 25A of the ASIO Act. However, the Law Council considers that these proposed paragraphs may limit the right the privacy under article 17 of the International Covenant on Civil and Political Rights (**ICCPR**),[53] particularly when considering that proposed paragraph 27E(2)(b) potentially authorises entry into an innocent third party's home. The Law Council recommends that proposed paragraph 27E(2)(b) of the SDA be amended so that access to third party premises, computer or communication in transit should be limited to cases where an eligible Judge or nominated AAT member considers it is necessary (rather than appropriate) in the circumstances to execute the warrant, having regard to the human rights of the relevant parties including their right to privacy. Paragraphs 25A(4)(aaa) and 25A(8)(e) of the ASIO Act should be subsequently be amended, as should the relevant proposed provisions in the Crimes Act and Customs Act.[54] These

[49] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 91. See Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 2 item 49, s 27A.
[50] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 2 item 49, s 27A(7).
[51] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 88.
[52] See also Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 3 item 3 (s 3F(2A)(c)(i), 3F(2D)(b) and 3F(2E) of the Crimes Act) and sch 4 item 4A (ss 199(4A)(c)(i), 199(4C)(b)), and sch 4 item 5 (s 199**B**(2)(c)(i) and 199B(4)(b) of the Customs Act).
[53] *International Covenant on Civil and Political Rights*, opened for signature, 999 UNTS 171 (entered into force 23 March 1976 art 17.
[54] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 sh 3 item 3 (ss 3F(2A)(c)(i), 3F(2D)(b) and 3F(2E) of the Crimes Act)) and sch 4 item 4A (ss 199(4A)(c)(i) and 199(4C)(b) of the Customs Act) and sch 4 item 5 (199**B**(2)(c)(i) and 199B(4)(b) of the Customs Act)).

amendments would ensure the proposed paragraphs which limit the right to privacy under the ICCPR are proportionate.[55]

Recommendation

- **Proposed paragraph 27E(2)(b), which authorises a computer access warrant to enter any premises for the purposes of gaining entry to, or exiting, the specified premises, be amended so that access to third party premises, computer or communication in transit should be limited to cases where an eligible Judge or nominated AAT member considers it is necessary (rather than appropriate) in the circumstances to execute the warrant, having regard to the human rights of the relevant parties including their right to privacy. Paragraphs 25A(4)(aaa) and 25A(8)(e) of the ASIO Act, proposed subparagraph 3F(2A)(c)(i), proposed subparagraph 3F(2D)(b) and proposed section 3F(2E) of the Crimes Act, and proposed subparagraphs 199(4A)(c)(i) and 199B(2)(c)(i), and proposed paragraphs 199(4C)(b) and 199B(4)(b) of the Customs Act should be subsequently be amended.**

Telecommunications interception under computer access warrants

Threshold

105. The Law Council notes that the proposal to attach telecommunications interception powers to the computer access warrants would involve a reduction in the threshold for telecommunications interception which does not appear to be justified in the Explanatory Memorandum to the Bill.

106. Proposed paragraph 25A(4)(b)[56] of the ASIO Act further expands the powers available under a computer access warrant by authorising the interception of a communication passing over a telecommunications system, if the interception is for the purpose of doing any thing specified in the warrant. The Explanatory Memorandum explains that this new power rectifies the current problem whereby ASIO can obtain a computer access warrant, but cannot obtain a telecommunications interception warrant which is needed under sections 9 and 9A of the TIA Act to establish computer access. According to the Explanatory Memorandum this system of requiring two warrants reduces the likelihood of a computer access warrant being validly executed, and increases administrative inefficiency.[57]

107. The thresholds for issuing a warrant under sections 9 or 9A of the TIA Act and section 25A (computer access warrant) and subsections 27A(3C)(g)-(h) (foreign intelligence warrants) and 27E(2)(d) (identified person warrants) of the ASIO Act, differ. To issue a telecommunications service warrant under sections 9 or 9A of the TIA Act the Attorney-General must be satisfied that a telecommunications service is

[55] Parliamentary Joint Committee on Human Rights *Guidance Note 1: Drafting statements of compatibility* (December 2014), 2.
[56] See also Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch 2 item 8 (s 27A(3C)(g)-(h) (foreign intelligence warrants under the ASIO Act)) and sch 2 item 9 (s 27E(2)(d) (identified person warrants under the ASIO Act).
[57] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 80.

being or is likely to be used by a person engaged in or likely to engage in activities prejudicial to security. To issue a computer access warrant under 25A of the ASIO Act the Attorney-General must be satisfied that the data will assist the collection of intelligence in respect of a matter that is important in relation to security. Therefore, by inserting proposed paragraph 25A(4)(ba) (computer access warrants), 27A(3B)(g)-(h) (foreign intelligence warrants) and 27E(2)(d) (identified person warrants) into the ASIO Act that allows for interception of communication passing over a telecommunications system, the threshold appears to be lowered from 'prejudicial to security' to 'a matter is important in relation to security'.

108. Telecommunication intercept warrants are issued in relation to the potential acts or activities of a person and the proposed computer access warrant is directed to the obtaining of data that is present on a computer without attributing the data present on the computer necessarily to the acts or activities of any particular person in placing the data on the computer. Nonetheless, there should be consistency in language and test regarding the threshold for access.

109. The Law Council does not consider that the potential lowering of the threshold has been demonstrated to be necessary and proportionate. The Law Council acknowledges that administrative efficiencies may be gained through a single warrant regime for computer access warrants. However, such efficiencies must not be achieved at the expense of privacy concerns relating to the potential intrusiveness of computer access warrants, and should only be adopted where appropriate safeguards exist.[58]

110. The Law Council therefore recommends that for ASIO a computer access warrant allowing the interception of a communication passing over a telecommunications system can only be authorised by the Attorney-General if the Attorney-General is satisfied that the telecommunications service is being or is likely to be used for purposes prejudicial to security.

111. Currently, under the TIA Act where a law enforcement agency applies to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service, the Judge or nominated AAT member must be satisfied that for example information that would be likely to be obtained by intercepting under a warrant communications made to or from the service 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.[59] Serious offences are generally include offences punishable by imprisonment for life or for a period or a maximum period of at least seven years under section 5D of the TIA Act. Telecommunications interception may also be available under the TIA Act for example under a named person warrant [60] which also requires an investigation into one or more serious offences or a control order warrant.[61]

112. However, under the proposed amendments to the SDA it is proposed to lower this threshold so that telecommunications interception may be permitted as part of a computer access warrant for a 'relevant offence' defined in section 6(1) of the SDA as a Commonwealth offence, or a State offence with a federal aspect, that is

[58] See Law Council of Australia, Submission No 23 to the Senate Committee on Legal and Constitutional Affairs, *Comprehensive Review of the Telecommunications (Interception and Access) Act 1979* (Cth) (14 March 2015), 41.
[59] *Telecommunications (Interception and Access) Act 1979* (Cth) s 46(1)(d).
[60] Ibid ss 46A, 46(4).
[61] Ibid s 46A(2A).

punishable by imprisonment for a minimum of three years, or an offence otherwise prescribed in section 6(1) or by regulations. This would be a significant increase in the powers of law enforcement agencies and does not appear to have been justified as a necessary and proportionate response.

113. In addition, there appears to be a lowering of thresholds in relation to control orders and telecommunications interception from what currently applies in the TIA Act context. For example, currently under paragraphs 46(6)(a) and (b) the Judge or nominated AAT member must not issue a warrant where a control order is in force in relation to another person, and the particular person is likely to communicate with the other person using the service unless he or she is satisfied that:

- the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person to whom the control order referred to in subparagraph (4)(d)(ii) relates; or

- interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

114. In the absence of sound justification to depart from the current thresholds relating to telecommunications interception access, these thresholds should be maintained for the purposes of the new computer access warrants.

Recommendation

- **While the Law Council recognising the different features of telecommunication intercept warrants and computer access warrants, are different, in the absence of evidence to suggest why amendments to existing thresholds in relation to telecommunications interception should be lowered, the Bill should be amended to retain the existing thresholds that apply for the purposes of the new computer access warrants in the ASIO Act and SDA. This requires for example that:**
    - **existing thresholds for ASIO a computer access warrant, foreign intelligence warrant or identified persons warrant allowing the interception of a communication passing over a telecommunications system can only be authorised by the Attorney-General if the Attorney-General is satisfied that the telecommunications service is being or is likely to be used for purposes prejudicial to security;**
    - **telecommunications interception under a computer access warrant should be limited to relevant offences under the SDA that are serious offences under the TIA Act; and**
    - **the Judge or nominated AAT member must not issue a warrant under the SDA where a control order is in force in relation to another person, and the particular person is likely to communicate with the other person using the service unless he or she is satisfied that the agency has exhausted all other practicable methods or interception of communications made to or from a telecommunications**

	service used or likely to be used by that person would not otherwise be possible.

Scope

115. The Law Council notes that the Bill would amend the ASIO Act and the SDA to allow the Attorney-General or a Judge or nominated AAT member to authorise telecommunications interception for the purpose of entering specified premises or gaining entry to or exiting specified premises. It is unclear why this power is necessary or justified.

Recommendation

- **In the absence of such justification, and if the telecommunications interception power in the new computer access warrants is to proceed, it should be limited to the purpose of obtaining access to 'relevant data' as defined for example under existing paragraphs 25A(4)(a) and 27E(2)(c) and (d) of the ASIO Act and proposed paragraphs 25A(4)(ab) of the ASIO Act and 27E(2)(c) of the SDA.**

Use of force

116. The Law Council is concerned that the interception capability under the new computer access warrants must allow the use of force by virtue of application of existing paragraphs 25A(5A)(a), 27A(2)(a) and 27J(3)(d) of the ASIO Act and by proposed paragraph 27E(6)(a) of the SDA. This would be a significant expansion of ASIO and law enforcement agency powers as currently interceptions warrants issued under Part 2-2 and Part 2-5 of the TIA Act do not allow the use of force. The Law Council does not consider that it has been demonstrated to be necessary or proportionate to authorise the use of force for the purpose of intercepting a telecommunication.

Recommendation

- **In the absence of adequate justification, the authorisation of the use of force should be prohibited for the telecommunications interception power in the new computer access warrants.**

Reporting requirements

117. There appears to be a disparity in reporting requirements which requires clarification. Under subsection 17(2) of the TIA Act, a report under subsection (1) in relation to a warrant issued under section 9A or 11B (named person warrants and named person warrants for the collection of foreign intelligence respectively) must include details of the telecommunications service to or from which *each intercepted communication* was made. There does not appear to be an amendment to subsection 17(2) of the TIA Act to ensure that there is a similar requirement for the new computer access warrants or section 34 of the ASIO Act or for proposed subsection 49(2B) of the SDA.

Recommendation

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

Protected and restricted information

118. The TIA Act and SDA include specific requirements for the use, storage and destruction of certain information.[62] However, such requirements are specifically to be excluded for the general computer access warrants that involve telecommunications interception. That is, the Bill proposes to amend the definition of 'restricted record' in the TIA Act to exclude the definition of 'general computer access intercept information'. It also proposes to amend the definition of 'protected information' in subsection 44(1) of the SDA to exclude 'general computer access intercept information'. The Law Council considers that this has not been demonstrated to be necessary or proportionate, particularly given the standards set by the TIA Act relating to the protection of such information.

Recommendation

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

Apparent inconsistency in emergency authorisations

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

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

121. The Law Council considers that consistency is desirable and that avoiding the prohibition on intercepting communications has not been justified.

Recommendation

- **The Bill should be amended to outline that telecommunications intercepts will not be permitted under emergency authorisations as is consistent with existing subsection 32(4) of the SDA.**

[62] See, for example, *Telecommunications (Interception and Access) Act 1979* (Cth) ss 31C, 79, 79AA and *Surveillance Devices Act 2004* (Cth) ss 3(c) and 46A.

Removal of computers or other things from premises

Scope

122. The Law Council considers that the temporary removal power is too broad as it would allow the Attorney-General or Judge or nominated AAT member to authorise the temporary removal of computers or other things from premises for the purpose of entering specified premises or gaining entry to or exiting specified premises.[63] It is unclear why this power is necessary or justified.

123. In the absence of such justification, and if the temporary removal power in the new computer access warrants is to proceed, it should be limited to the purpose of obtaining access to 'relevant data' under existing paragraphs 25A(4)(a) and 27E(2)(c) and (d) of the ASIO Act and proposed paragraphs 25A(4)(ab) of the ASIO Act and 27E(2)(c) of the SDA.

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

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

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

127. A maximum time limit should be placed on the period of removal.

Recommendations

- **In the absence of adequate justification, and if the temporary removal power in the new computer access warrants is to proceed, it should be limited to the purpose of obtaining access to 'relevant data' under existing paragraphs 25A(4)(a) and 27E(2)(c) and (d) of the ASIO Act and proposed paragraphs 25A(4)(ab) of the ASIO Act and 27E(2)(c) of the SDA.**
- **The criteria for what objects may be temporarily removed should be clearly set out in the legislation to ensure that there is a rational connection with the legitimate objective of the legislation.**
- **A maximum time limit should be placed on the period of removal.**

Reporting requirements

128. Under existing subsection 34(1) of the ASIO Act the Director-General is required to provide to the Attorney-General in respect of each warrant issued under the Division a report in writing on the extent to which the action taken under the warrant has assisted the ASIO in carrying out its functions. Subsection 34(2) of the ASIO Act also requires reports on removals that may cause a material interference with, or

[63] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 sch 2 item 4 (s 25A(4)(ab) of the ASIO Act)) and sch 2 item 9 (s 27E(2)(d) of the SDA)). See also *Australian Security Intelligence Organisation Act 1979* (Cth) ss 25A(4)(a) and 27E(2)(c)-(d).

interruption or obstruction of the lawful use by other persons of a computer or other electronic equipment, or a data storage device. Items 14 and 15 of Schedule 2 of the Bill would amend subsection 34(2) of the ASIO Act to extend this reporting requirement to material interference, interruption or obstruction caused by a temporary removal under the concealment of access powers under proposed new subsections 25A(8), 27A(3C) and 27E(6). However, there do not appear to be general requirements to report on all removals under the general computer access warrant powers but only those that may cause a material interference with, or interruption or obstruction of the lawful use by other persons of a computer or other electronic equipment, or a data storage device under subsection 34(2) of the ASIO Act. In practice, it may be difficult to determine when a removal causes a material interference, interruption or obstruction as this threshold may be met given the frequency of use of a computer in ordinary daily life. Nonetheless, to aid clarity, the Law Council considers that there should be a requirement to aid transparency to report on all temporary removals under computer access warrants.

Recommendation

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

Issuing of computer access warrants – law enforcement

129. Computer access warrants under proposed section 27D(1)(b)(ix) allow the warrant to identify a target 'by name or otherwise'. As the 'otherwise' is not defined in the Bill both the law enforcement users of the warrant and the issuing authority may have difficulty in determining the exact requirements. This should be addressed in the Bill prior to enactment.

Recommendation

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

Concealment

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

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

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

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

    (d) the interception of telecommunications; and

(e) other things reasonably incidental to these activities.

Automatic concealment authorisation

131. These individual concealment activities do not require approval from the Attorney-General or Director-General or a Judge or nominated AAT member but instead are authorised automatically by a computer access warrant.

132. These powers seem to be inconsistent with existing powers under paragraphs 25A(4)(c) and 27E(2)(f) of the ASIO Act which allow the Attorney-General or Director-General to specifically authorise certain concealment activities for the duration only of the particular warrant.

133. The Law Council considers that it is important to have the Attorney-General or Director-General or Judge or nominated AAT member authorise specific concealment activities to avoid unnecessary or disproportionate use of the powers. Requiring a specific authorisation will also ensure that ASIO or the relevant law enforcement agency carefully plan what powers will be required to meet the relevant intelligence or law enforcement objective. The Bill should be amended accordingly.

Certain acts not authorised

134. The proposed new concealment provisions in the ASIO Act and the SDA also do not include the current safeguards regarding 'certain acts not authorised' which apply to the current concealment powers under the ASIO Act.[64] That is, they do not appear to include the limitations on any damage or loss caused by the concealment activities. The Explanatory Memorandum does not appear to justify why such safeguards have not been carried over to the new provisions. The Law Council considers that these safeguards should be present for any new concealment powers to assist in the proportionality of the measures.

Duration

135. As noted, concealment activities can be done 'at any time while the warrant is in force or within 28 days after it ceases to be in force'. However if nothing has been done within the 28 day period to conceal the fact a computer has been accessed, they may be authorised 'at the earliest time after the 28-day period at which it is reasonably practicable' to conceal access to a computer under warrant.[65] The Explanatory Memorandum notes that 'it is sometimes impossible' to complete the process of concealing activities within 28 days of the warrant expiring.[66]

136. The Law Council is concerned that the absence of a time limit by which concealment of access powers may be exercised may authorise privacy-intrusive activities in the absence of the reasonable grounds threshold which underpin the initial warrant.

137. The Law Council therefore recommends that proposed paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) of the ASIO Act and proposed paragraphs 27E(7)(k) of the SDA should not proceed. In the alternative, ASIO should be able to apply to the Attorney-General (or in the case of an identified person warrant the Director-

---

[64] *Australian Security Intelligence Organisation Act 1979* (Cth) s 27E(7).
[65] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 sch 2 item 7 (s 25A(8)(k) of the ASIO Act), sch 2 item 8 (s 27A(3C)(k) of the ASIO Act), sch 2 item 12 (s 27E(6)(k) of the ASIO Act), and sch 2 item 49 (s 27E(7)(k) of the SDA).
[66] Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, 99.

General) for an extension of time with a maximum limit where it is necessary for the concealment of access. Indeed, the Bill allows for this in relation to law enforcement agencies under proposed section 27F of the SDA.

Recommendations

- **Proposed paragraphs 25A(8)(k), 27E(6)(k) and 27A(3C)(k) of the ASIO Act and proposed paragraphs 27E(7)(k) of the SDA should not proceed.**
- **In the alternative, 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.**

New section 64AD: compulsory assistance to law enforcement relating to data

138. Proposed section 64A of the SDA would permit a law enforcement officer to apply to an eligible Judge or AAT member for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to access data held in a computer subject to a computer access warrant.

139. The eligible Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that access to data is necessary in the course of the investigation to enable evidence of the commission of the offences or identity or location of the offenders.

140. In addition, the person specified in the order must be:

(a) reasonably suspected of having committed any of the offences to which the warrant or emergency authorisation relates;

(b) the owner or lessee of the computer or device;

(c) an employee of the owner or lessee of the computer or device;

(d) a person engaged under a contract for services by the owner or lessee of the computer or device;

(e) a person who uses or has used the computer or device, or

(f) a person who is or was a system administrator for the system including the computer or device.

141. This is different to the requirements for the proposed compulsory assistance powers in new section 34AAA from the ASIO Act where the suspected activities prejudicial to security do not need to be related to the assistance order (see below).

142. However, like proposed section 34AAA of the ASIO Act, in proposed section 64AD of the SDA it is unclear whether the 'specified person' is only a natural person, or could also include a 'legal person' such as a body corporate, or a representative thereof.

143. Consideration should also be given to whether further safeguards should be required for section 64AD to limit the possibility of arbitrary detention (as discussed in more detail below in relation to section 34AAA of the ASIO Act).

Recommendation

- **Proposed section 64AD of the SDA should clearly outline whether the 'specified person' is a natural person or a legal person.**

Disproportionate penalties

144. Under proposed sections 64A of the SDA and 34AAA of the ASIO Act a law enforcement officer or the Director-General may request an order requiring a specified person to provide information or assistance that is reasonably and necessary to fulfil a warrant. This includes requiring a person to provide information or assistance to a law enforcement officer or ASIO to allow them to access or copy data held on a computer, or convert data to an intelligible form.[67] The penalty for failing to comply with an assistance order is five years imprisonment or 300 penalty units, or both, under proposed section 34AAA of the ASIO Act, and a maximum of ten years imprisonment under proposed section 64A of the SDA. Under proposed section 64A a law enforcement officer may apply to an eligible Judge or nominated AAT member for an order. Under proposed section 34AAA the Director-General need only request the Attorney-General to make an order; there is no requirement for a Judge or AAT member to make the order.

145. Under proposed sections 64A and 34AAA it is an offence for a person to fail to comply with an assistance order where the relevant warrant relates to a serious offence. The penalty for failing to comply is maximum ten years imprisonment, however a 'serious offence' under the Crimes Act can be one that is punishable by two years' imprisonment. This means that a person who fails to comply with an assistance order where the warrant in question relates to an offence attracting a two-year imprisonment penalty, may be penalised for a maximum ten years imprisonment. This may result in criminal sentences that are disproportionate to the gravity of any offence committed and therefore may potentially engage the right of a person to not be deprived of their liberty unlawfully or arbitrarily.[68] The Law Council recommends that the PJCIS consider reducing the penalty available under proposed sections 64A and 34AAA of the Bill to be proportionate to the penalties relating to a 'serious offence' under the Crimes Act.

Privilege against self-incrimination

146. The Law Council notes the potential for the assistance orders relating to computer access warrants under proposed section 34AAA of the ASIO Act and section 64A of the SDA to impinge on the privilege against self-incrimination. A 'specified person' can be given an assistance order if it is reasonably suspected they are involved in an offence to which the warrant relates, or they are the owner, employee of the owner, engaged in a contract with the owner, have used, or are the system administrator, of the computer device to which the warrant relates, and they have

[67] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 sch 2 item 114 (s 64A(1)) and sch 5 item 3 (s 34AAA(1)).
[68] *International Covenant on Civil and Political Rights*, opened for signature, 999 UNTS 171 (entered into force 23 March 1976 art 9(1).

relevant knowledge of the computer or device.[69] There is the potential that a specified person who provides ASIO or a law enforcement officer with access to a computer device, such as through a computer or phone password under an assistance order, may provide information that incriminates them.

147. The common law privilege against self-incrimination provides that a person cannot be required to answer questions or produce material which may tend to incriminate them.[70] The common law privilege against self-incrimination and against penalty is a substantive right of long standing, applicable to criminal and civil penalties and forfeiture. It is deeply ingrained in the common law and is not to be taken to be abrogated by statute except in the clearest terms.[71] Its protection is required by the ICCPR[72] and is protected under Australia's legislative framework.[73]

148. The *Guide to Framing Commonwealth Offences* (**Guide**) published by the Attorney-General's Department, suggests that 'where the privilege against self-incrimination is to be overridden, it is usual to include a 'use' immunity or a 'use and derivative use' immunity provision, which provides some degree of protection for the rights of individuals'.[74] The Guide explains use and derivative use immunity in the following terms:

- *'use' immunity – self-incriminatory information or documents provided by a person cannot be used in subsequent proceedings against that person, but can be used to investigate unlawful conduct by that person and third parties, and*
- *'derivative use' immunity – self-incriminatory information or documents provided by a person cannot be used to investigate unlawful conduct by that person but can be used to investigate third parties.*[75]

149. The Law Council considers that consistent with the Guide, where proposed section 34AAA of the ASIO Act and 64A of the SDA appear to override the privilege against self-incrimination, use and derivative use immunities should be available.

[69] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 sch 2 item 114 (s 64A(2)(d)-(e)) and sch 5 item 3 (s 34AAA(2)(c)-(d)).
[70] *Sorby v Commonwealth* (1983) 152 CLR 281; *Pyneboard Pty Ltd v Trade Practices Commission* (1983) 152 CLR 328.
[71] *Smith v Read* (1736) 1 Atk 526 at 527; [26 ER 332]; *R v Associated Northern Collieries* (1910) 11 CLR 738 at 742, 744; *Sorby v Commonwealth* (1983) 152 CLR 281, at 309–310 and 316; *Daniels Corporation International Pty Ltd v ACCC* (2002) 213 CLR 543 at 554; *Rich v ASIC* (2004) 220 CLR 129 at 141- 143.
[72] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 14(3)(g).
[73] *Evidence Act 1995* (Cth), 1995 (NSW), 2001 (Tas), 2008 (Vic), 2011 (ACT), *Evidence (National Uniform Legislation) Act* (NT), ss128, 128A; *Human Rights Act 2004* (ACT), s22(2)(i); *Charter of Human Rights and Responsibilities Act 2006* (Vic), s25(2)(k). See also *Australian Securities and Investments Commission Act 2001* (Cth), s68; *Banking Act* 1959 (Cth), s52F; *Competition and Consumer Act 2010* (Cth), ss155(7), 155B, 159; *Corporations Act 2001* (Cth), ss597(12) and (12A), *Work Health and Safety Act 2011* (Cth), s172; *Royal Commissions Act 1903* (Cth), ss6A (3), (4).
[74] Attorney General's Department, *Guide to Framing Commonwealth Offences,* (September 2011), 96, [9.5.4].
[75] Ibid.

Recommendations

- **The PJCIS consider reducing the penalty available under proposed sections 64A and 34AAA of the Bill to be proportionate to the penalties relating to a 'serious offence' under the Crimes Act.**
- **Proposed sections 34AAA and 64A be amended to include a 'use' immunity and a 'derivative use' immunity.**

Compensation

150. The Law Council notes that while the Bill provides for compensation for providers assisting agencies, there is no requirement for the Commonwealth to pay compensation for loss or injury resulting from the unlawful use of a computer access warrant. This should be rectified.

Recommendation

- **Section 64 of the SDA be amended ensure liability by the Commonwealth to pay compensation for loss or injury resulting from the unlawful use of a computer access warrant.**

Mutual Assistance in Criminal Matters

151. The Bill would amend MACMA to enable foreign authorities to make a request to the Attorney-General to authorise an eligible domestic law enforcement officer to apply for, and execute, a computer access warrant for the purposes of obtaining evidence to assist in a foreign investigation or investigative proceeding.

152. Proposed section 15CC would enable the Attorney-General to, in their discretion, authorise an eligible law enforcement officer to apply for a computer access warrant under the SDA if satisfied that for example the investigation or investigative proceeding relates to a criminal matter involving an offence against the law of a foreign country punishable by a maximum penalty of imprisonment for 3 years or more, imprisonment for life or the death penalty.

153. The Law Council has previously called for an independent review of the MACMA to ensure that Australia is complying with fundamental rule of law principles and its international obligations.

154. Subsection 8(1A) of the MACMA requires the Attorney-General to refuse a mutual assistance request in death penalty cases where a person has been arrested or detained. Subsection 8(1A) also permits the Attorney-General to provide assistance in death penalty cases where they are satisfied that 'special circumstances' exist. 'Special circumstances' are not defined in the MACMA.

155. Clarity around what is meant by 'special circumstance' in the legislation would assist in providing the community with reassurance that mutual assistance will only be provided in appropriate cases. For example, special circumstances may include where the evidence would assist the defence, or where the foreign country undertakes not to impose or carry out the death penalty.

156. Consideration should be given to amending the MACMA to clearly define 'special circumstances' for the purposes of mutual assistance in cases where an offence in a

foreign country may be punishable by the death penalty. Otherwise, there is nothing in the legislation itself that would limit the Attorney-General's discretion to determine what would consist of a 'special circumstance'. The breadth of this discretion may create a risk, despite good intentions, that Australian assistance prior to arrest or detention may lead to the imposition of the death penalty.

Recommendations

- **An independent review of the MACMA should be conducted to ensure that Australia is complying with fundamental rule of law principles and its international obligations; and**
- **Consideration should be given to amending the MACMA to clearly define 'special circumstances' for the purposes of mutual assistance in cases where an offence in a foreign country may be punishable by the death penalty.**

Schedule 3 and 4 – Search Warrants issued under the Crimes Act and Customs Act

157. Schedules 3 and 4 are complementary and amend the Crimes Act and Customs Act respectively. Schedule 4 contains additional, quite detailed, material about the requirements for the issue of a warrant under the Customs Act, presumably because the additional material was not needed for the Crimes Act.

158. In general terms, Schedule 3 would amend the Crimes Act to expand the powers of criminal law enforcement agencies to collect evidence from electronic devices found during the execution of a search warrant. It would allow law enforcement agencies to:

(a) overtly or remotely use specialist equipment to seize or search computers;

(b) access 'account based data' from a computer under a search warrant to enable access to information on an online account; and

(c) increase the time for temporary removal of an electronic device to obtain evidentiary material from 14 days to 30 days.

159. Schedule 4 would amend the Customs Act to increase the Australian Border Force's ability to collect evidence from electronic devices under warrant in person or remotely. This includes:

(a) a new power to request a search warrant to be issued in respect of a person for the purposes of seizing a computer or data storage device;

(b) increasing the penalties for not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force; and

(c) increasing the timeframes for the examination of electronic devices moved under a warrant from 72 hours to 30 days.

160. The provisions are comprehensive insofar as they extend to the search and seizure of computers and electronic storage devices, to the possessors of such devices and to those who are 'likely' to use them (or in the case of deceased persons of interest,

those who were likely to have used them). They also extend to devices and communications (including communications in progress) that might be expected to provide assistance in identifying and obtaining evidential material from that or other devices. Entries on electronic devices may be for example altered or deleted, if necessary to enable the identification of evidential material in that or another device. The collection of information may also be done remotely.

161. Schedules 3 and 4 would give extensive powers to investigators for direct and indirect intervention in private communications.

162. The Law Council notes that it is positive that in all cases judicial warrants are required and action is specifically circumscribed by the terms of the warrant.

163. However, the Law Council reiterates its concerns regarding the privacy impact on third parties that equally apply to these provisions.

164. The Law Council also notes that action may be taken to assist in the enforcement of a law applying in a foreign jurisdiction, which, inter alia, raises the spectre of Australian assistance in the enforcement of foreign law that might result in a death penalty. The Law Council reiterates its view as noted above in relation to the MACMA.

Schedule 5 – Civil immunities for voluntary assistance to ASIO

165. Proposed new subsection 21A(1) of the ASIO Act would confer 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 new subsection 16(1A). This proposed internal authorisation would represent a significant expansion of power as currently only the Attorney-General may confer a civil or criminal immunity on participants in a SIO.

166. Proposed subsection 21A(1) would provide that if the Director-General or their delegate requests a person or body to engage in conduct that the Director-General or their delegate is satisfied is likely to assist ASIO in the performance of its functions and:

(a) the person engages in the conduct in accordance with the request; and

(b) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and

(c) the conduct does not result in significant loss of, or serious damage to, property the person or body is not subject to any civil liability for, or in relation to, that conduct.

167. The Law Council does not consider that the internal authorisation for the conferral of civil immunity has been demonstrated to be necessary and proportionate. In the absence of such evidence, the conferral of civil immunity powers should be by the Attorney-General.

168. The Law Council reiterates its view that proposed sections 317G and 317ZJ be amended to include limitations on the conferral of civil liability for providers who

comply with a TAR, TAN or TCN so that civil immunity is not conferred if the conduct results in significant loss of, or damage to, property, economic loss or physical or mental harm or injury (in line with proposed section 21A of the ASIO Act); and to include limitations and exceptions, to the extent possible that reflect those available in the controlled operations scheme and appropriately modified as required for intelligence agencies.

169. 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.

170. Further, it is not clear how the voluntary assistance provided to ASIO civil immunity provisions in proposed subsection 21A relate to the provisions for a TAR in Schedule 1 of the Bill, including civil immunity under a TAR. Clarification should be provided as to the intended relationship between the two immunities.

171. The immunity of civil liability does not cover conduct that results in significant loss of, or serious damage to, property but may arguably capture conduct that causes:

(a) economic loss; or

(b) physical or mental harm or injury which might otherwise constitute negligence.

172. It is critical that third parties are not deprived of a legal remedy for these factors. Accordingly, the Law Council recommends an amendment to the Bill to ensure that the immunity of civil liability does not cover conduct that causes economic loss or physical or mental harm or injury which might otherwise constitute negligence. Alternatively, it must be clear on the face of the legislation that an aggrieved person would have a legally enforceable remedy against ASIO.

Recommendations

- **In the absence of such evidence, the conferral of civil immunity powers for voluntary assistance to ASIO should be by the Attorney-General.**
- **Where ASIO would otherwise require Ministerial authorisation or approval under the ASIO Act, it should not be able to make a voluntary assistance request.**
- **Clarification should be provided as to the intended relationship between the two immunities.**
- **The Bill be amended to ensure that the immunity of civil liability does not cover conduct that causes economic loss or physical or mental harm or injury which might otherwise constitute negligence. Alternatively, it must be clear on the face of the legislation that an aggrieved person would have a legally enforceable remedy against ASIO**.

Procedural matters

173. The Law Council considers that the procedural framework surrounding requests made under new subsection 21A(1) and the associated immunity from civil liability should be improved to aid transparency and accountability as per the recommendation below.

Recommendations

- **The procedural framework surrounding requests made under new subsection 21A(1) and the associated immunity from civil liability should be improved to aid transparency and accountability by making it clear:**
  - **that compliance with a request is voluntary (as proposed for subsection 317HAA(1) of the Telecommunications Act);**
  - **how long the request will be in force with a maximum statutory period applying;**
  - **that a voluntary assistance provided to ASIO request does not cover ongoing requirements for assistance;**
  - **that oral requests should be followed by a written record to the person as soon as reasonably practicable;**
  - **the manner in which such requests may be varied or revoked; and**
  - **the manner in which there are reporting requirements under the provisions. The Law Council considers that there should be annual reporting to the Parliament on the number of times the provision is used; the kinds of assistance requested and provided; and the extent to which the civil immunity provision did not apply.**

New section 34AAA: compulsory assistance to ASIO relating to data

174. Under proposed new section 34AAA of the ASIO Act the Director-General of Security may request the Attorney-General to issue an order to a specified person to provide information or assistance to ASIO that is 'reasonable and necessary' so that ASIO may access,[76] copy[77] or convert[78] data held in, or accessible from a certain computer or data storage device that has been accessed under special powers warrants including:

- computer access warrants;
- search warrants;
- surveillance warrants; and

[76] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill sch 5 item 3 (s 34AAA(1)(a)).
[77] Ibid s 34AAA(1)(b).
[78] Ibid s 34AAA(1)(c).

- seized from individuals subjects to questioning or questioning and detention warrants.

175. The processes for making orders under this new section are modelled on section 3LA of the Crimes Act, but take account of ASIO's functions and the fact that the Attorney-General generally authorises ASIO warrants, rather than a judicial officer.

176. Proposed paragraph 34AAA(2)(c) applies to a specified person who:

(a) has a link to the computer or device;[79] or

(b) is reasonably suspected of being involved in activities that are prejudicial to security.[80]

177. It is unclear whether the 'specified person' is only a natural person, or could also include a 'legal person' such as a body corporate, or a representative thereof.

178. The threshold in proposed subparagraph 34AAA(2)(c)(i) that a person is reasonably suspected of being 'involved in' activities that are prejudicial to security appears to be very low. There seems to be no requirement for the person to know or intend to be involved in the prejudicial activities. Involvement could then include being a service provider who has no knowledge of the uses to which the end-user may put their products or services.

179. There appears to be an inconsistency between the new section 34AAA(2)(c)(i) and section 3LA(2)(b)(i) of the Crimes Act. Where the latter requires the magistrate to reasonably suspect the person of having committed the offence stated in the relevant warrant the new ASIO provision does not require the suspected prejudicial activities to be related to the assistance order.

180. The Explanatory Memorandum does refer to 'a target or the target's associate' being required to give 'a password, pin code, sequence or fingerprint necessary to unlock a phone' so it may be the case that the inconsistency is unintended. The legislation should make the link between the person subject of the assistance order and the security matter explicit.

181. New subsection 34AAA(3) outlines procedural requirements that apply if the relevant computer or data storage device is not on premises in relation to which a warrant is in force. These requirements include:

- the specification of the period of time in which the person must provide information or assistance;
- the place at which they must do so;
- and any other conditions determined by the Attorney-General.

182. It is not clear why proposed subsection 34AAA(3) only applies to computers not on the premises, but instead to all computers subject of the relevant warrant.

183. Proposed subsection 34AAA(4) creates offences for persons subject to assistance orders who contravene requirements.

[79] Ibid s 34AAA(2)(c)(ii)-(vi).
[80] Ibid 34AAA(2)(c)(i).

184. Proposed section 34AAA appears to be omitting any requirements for record keeping, cessation of activities, and destruction of material not relevant to the performance of ASIO's functions.

185. Such provisions are important to allow for appropriate oversight mechanisms, and to ensure the preservation of privacy for individuals where their activities are not relevant to security.

186. Other ASIO powers are subject to legislative requirements to keep appropriate records,[81] cease activities where the grounds for these are no longer in existence[82] and the destruction of information not relevant to security.[83]

187. As the proposed new 34AAA powers are not a 'warrant' the Ministerial reporting requirement under existing section 34 powers would not apply. The new provisions should have similar reporting requirements integrated into section 34.

Recommendations

- **Proposed section 34AAA of the ASIO Act should clearly outline whether the 'specified person' is a natural person or a legal person.**
- **Proposed subparagraph 34AAA(2)(c)(i) should require that a person is knowingly and intentionally involved in activities that are prejudicial to security.**
- **The legislation should make the link between the person being subject of the assistance order and the security matter explicit.**
- **The Explanatory Memorandum should explain why only computers and storage devices not on the premises are subject to 34AAA(3).**
- **Proposed section 34AAA should include adequate record keeping requirements. reporting requirements, instructions for the cessation of activities and destruction of materials at least consistent with other parts of the ASIO Act.**
- **The new provisions should have similar reporting requirements integrated into section 34.**

Informing the person subject to the order

188. It is notable that new section 34AAA does not outline how the specified person is to be advised of her or his new obligation and the time period for which thee obligations apply. This is inconsistent with the provisions of new Part 15 of the Telecommunications Act that govern the duration and compliance period in relation to TARs, and TANs and TCNs.

Recommendation

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

[81] *Australian Security Intelligence Organisation Act 1979* (Cth) s 32(4).
[82] Ibid s 30.
[83] Ibid s 31.

Complying with the order amounting to detention

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

190. The Law Council notes that 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.

191. While proposed section 64AD of the SDA (discussed above) requires judicial authorisation, consideration should also be given to whether the safeguards in relation to this provision could be improved to guard against arbitrary detention.

Recommendation

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

Questioning and Questioning and Detention warrants

192. It is unclear how the requirement for a person to attend a place and provide information or assistance under a section 34AAA order interacts with ASIO's compulsory questioning and detention powers under Division 3 of Part III of the ASIO Act, or TANs issued by ASIO under the proposed amendments to the Telecommunications Act in Schedule 1 of the Bill.

193. Under proposed subparagraph 34AAA(1)(a)(ix) orders may be issued to compel assistance or information in relation to accessing data held in, or accessible from, a computer or data storage device that has been seized during a search of a person

being detained under a questioning warrant or a questioning and detention warrant (section 34ZB).

194. This raises the issue of a person being subject to oppression through being the subject of multiple coercive powers to obtain information. Where there is a possibility of a person being subject to multiple concurrent compulsion orders, particularly strict oversight and accountability arrangements should be in place. There should be requirements to guard against oppressive use of multiple coercive powers to obtain particular information.

Recommendation

- **There should be requirements to guard against oppressive use of multiple coercive powers to obtain particular information.**

Human rights considerations

195. The Law Council has not had the opportunity to conduct a detailed human rights analysis of the Bill. Nonetheless, it appears that a number of the Bill's provisions engage important human rights obligations, including the following:

- Proposed section 317ZG which states that a designated communications provider must not be required to implement or build a systemic weakness or systemic vulnerability into a form of electronic communication, nor prevented from rectifying a systemic weakness or vulnerability in a form of electronic protection engages rights to privacy and freedom of opinion and expression.[84]
- The breadth of the proposed new 'industry assistance framework' under the Bill, which includes the operation of TARs, TANs and TCNs, to allow law enforcement and national security agencies to compel designated communications providers to do a range of acts or things, engages the right to privacy.[85]
- The new computer access warrants regime which enables the interception of communications for the purpose of executing a computer access warrant, permits the temporary removal and return of a computer or thing from a premises for the purpose of executing a warrant, and authorises agencies to do things that conceal access to a computer, including after the expiry of a warrant, engages the right to privacy.
- Proposed sections 64A and 34AAA may impact on the right not to be detained arbitrarily[86] and the right to humane treatment in detention.[87]
- Proposed sections 34AAA amending the ASIO Act (compulsory assistance relating to access to data) and 64A amending the SDA may interfere with the right against self-incrimination.[88]

196. The United Nations Human Rights Committee has confirmed that where a State party makes any restrictions on rights under the ICCPR which are derogable, it must 'demonstrate their necessity' and only take 'such measures as are proportionate to

[84] *International Covenant on Civil and Political Rights*, opened for signature, 999 UNTS 171 (entered into force 23 March 1976 arts 17 and 19.
[85] Ibid art 17.
[86] Ibid art 9(1).
[87] Ibid art 10.
[88] Ibid art 14(3)(g).

the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights'.[89]

197. Since its establishment by the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth), the Parliamentary Joint Committee on Human Rights (**PJCHR**) has consistently applied a proportionality analysis to provisions which appear to limit human rights. Where a provision appears to limit rights, the PJCHR considers three key questions:

- whether and how the limitation is aimed at achieving a legitimate objective;
- whether and how there is a rational connection between the limitation and the objective; and
- whether and how the limitation is proportionate to that objective.[90]

198. To demonstrate that a limitation is permissible, proponents of legislation must provide reasoned and evidence-based explanations as to how the measures are likely to be effective in achieving the objective sought.[91]

199. To determine whether there is a rational connection between a limitation and its objective, the Attorney-General Department's guidance for those who have a role in Commonwealth legislation, policy and programs suggests the following questions may be useful:

- Will the limitation in fact lead to a reduction of that problem?
- Does a less restrictive alternative exist, and has it been tried?
- Is it a blanket limitation or is there sufficient flexibility to treat different cases differently?
- Has sufficient regard been paid to the rights and interests of those affected?
- Do safeguards exist against error or abuse?
- Does the limitation destroy the very essence of the right at issue?[92]

200. In considering whether a limitation on a right is proportionate to its objective, the PJCHR has identified some factors that might be relevant to include:

- whether there are other less restrictive ways to achieve the same aim;
- whether there are effective safeguards or controls over the measures, including the possibility of monitoring and access to review;
- the extent of any interference with human rights – the greater the interference the less likely it is to be considered proportionate; and

---

[89] United Nations Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, 2187th mtg, UN Doc CCPR/C/21/Rev.1/Add.13 (26 May 2004), [6].

[90] Parliamentary Joint Committee on Human Rights, *Annual Report 2012-2013* (December 2013) [1.53]; Parliamentary Joint Committee on Human Rights, *Guide to Human Rights* (June 2015) [1.15]. These are also reflected in the Law Council of Australia, *Policy statement on human rights and the legal profession: Key principles and commitments* (May 2017).

[91] Parliamentary Joint Committee on Human Rights *Guidance Note 1: Drafting statements of compatibility* (December 2014), 2.

[92] Attorney-General's Department, 'Permissible limitations' Australian Government <https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/Permissiblelimitations.aspx>.

- whether the measure provides sufficient flexibility to treat different cases differently or whether it imposes a blanket policy without regard to the merits of an individual case.[93]

201. Accordingly, the Law Council recommends that the Bill not be enacted until these issues, and any other issues identified by the PJCHR in relation to the Bill, have been subject to a structured proportionality analysis.

Recommendation

- **The Bill should not be enacted until any human rights issues identified by the PJCHR in relation to the Bill have been addressed.**

[93] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Guide to Human Rights* (2015) [1.21].