Law Council
OF AUSTRALIA

# Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

**Department of Home Affairs**

**10 September 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 is grateful for the assistance of the Law Institute of Victoria, the Privacy and Data Committee of the Law Society of New South Wales, the Privacy Committee of the Business Law Section of the Law Council and the Law Council's 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 Department of Home Affairs' (**the Department**) Consultation on the Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**the Exposure Draft Bill**).

2. The Law Council acknowledges that there is significant value to public safety in allowing law enforcement authorities 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 cybercrimes which occur across multiple jurisdictions.

3. The Law Council recognises that a principal objective of the Exposure Draft 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 for legislative clarity and certainty (given the diverse range of agencies that may utilise these powers and the significant expansion in the range and nature of entities that will be relevantly subject to complex law enforcement legislation for the first time) and the need for reasonably transparent and verifiably reliable safeguards and controls. The Exposure Draft Bill does include some useful controls and safeguards. However, they are limited in scope and more limited in transparency and oversight. The Law Council supports many of the proposed safeguards, including continuing to require agencies to seek a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), *Surveillance Devices Act 2004* (Cth) (**SDA**) or *Crimes Act 1914* (Cth) (**Crimes Act**). However, the powers as conferred go far beyond the rationale for operation of the proposed enhanced powers of agencies as stated in the commentary provided by the Department.

4. According to the Department, the Exposure Draft 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. The Exposure Draft Bill intends to address these threats by introducing a suite of measures that will improve the ability of agencies to access intelligible communications content and data. In fact, the measures proposed go far beyond these threats, to include assisting the enforcement of *any* criminal laws in force in *any* foreign country, enforcing laws imposing a pecuniary penalty (being many, if not most, laws, including local government authority and council by-laws), and any exercise of any power under any law protecting the public revenue (for example, proposed paragraph 317L(2)(c)).[1] According to the Exposure Draft Bill's Explanatory Memorandum, three distinct reforms will help achieve improved access:

    a. enhancing the obligations of domestic providers to give reasonable assistance to Australia's key law enforcement and security agencies and, for the first time, extending assistance obligations to offshore providers supplying communications services and devices in Australia;

[1] The Law Council notes note that in each case the power would only be exercisable by an agency listed as an 'interception agency' in proposed section 317B, but note that this will include Federal, State and Territory Police Forces acting in aid of other Government agencies. We do 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.

b. introducing new computer access warrants for law enforcement that will enable agencies/authorities to covertly obtain evidence directly from a device; and

c. strengthening the ability of law enforcement and security authorities to overtly access data through the existing search and seizure warrants.

5. The Law Council considers that the primary issues that arise from the Exposure Draft Bill relate to:

- the purpose of the Exposure Draft Bill;
- the scope of the Exposure Draft Bill as it relates to entities;
- the scope of the Exposure Draft Bill as it relates to activities;
- managing compliance costs;
- protection of individual privacy;
- accountability/oversight; and
- comparison with other jurisdictions.

6. The Law Council has considered the positive and negative aspects of the Exposure Draft Bill in relation to each of the primary issues that it suggests arise from the Exposure Draft Bill, and provides the following comments and recommendations.

# The purpose and operation of the Exposure Draft Bill

7. In relation to the purpose of the Exposure Draft Bill, the Law Council acknowledges that there is significant value to public safety in allowing law enforcement authorities 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 cybercrimes which occur across multiple jurisdictions, and that Australia has ratified the Budapest Convention on Cybercrime.[2]

8. The Law Council echoes the guiding principle that the 'protection of privacy should continue to be a fundamental consideration in and the starting point for any legislation providing access to telecommunications for security and law enforcement purposes'.[3]

9. To given substance to this principle, it should be stated that each interference in the fundamental human right to privacy should be considered and weighted against any perceived imperative to protect society from significant threats and to protect the personal safety of individuals. This statement would assist in achieving an appropriate balance to ensure that the opening by decryption or removal of password protection of an otherwise encrypted or protected communication is not arbitrary.[4]

---

[2] Convention on Cybercrime, opened for signature 23 November 2011, ETS No. 185 (entered into force 1 July 2004).

[3] Anthony Blunn, *Report of the Review of the Regulation of Access to Communications, Attorney-General's Department* (2005), 5. See also Law Council of Australia, Submission No 21 to the Parliamentary Joint Committee on Law Enforcement, *Inquiry on the Impact of New and Emerging ICT on Australian law enforcement agencies*, 6 February 2018, 7.

[4] Article 17 of the *International Covenant on Civil and Political Right*s of 1966, stating that (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; and (2) Everyone has the right to the protection of the law against such interference or attacks.

10. The protection of the fundamental human right to privacy should be weighed against the expansion of purposes (or 'relevant objectives' as variously defined in the Exposure Draft Bill) which are used to carve out exclusions to the prohibition on access to communications.

11. The Law Council was informed by the Department that the Exposure Draft Bill is not intended to allow a relevant agency to view the content of a communication or electronic record in any circumstance where viewing of that content requires a warrant or authorisation. In other words, the power to request or require decryption (or an individual to facilitate opening up a password protected device) does not displace the need for an agency to obtain lawful authority to view the content of a communication or electronic record. The Law Council suggests that this fundamental limitation must be expressly stated in the legislation. The limitation is only partially given effect by a reader interpreting the drafting in proposed section 317ZH, which only references a number of Federal Acts. The 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 Exposure Draft 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 Exposure Draft 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.

12. The Law Council accepts that a law enforcement agency should not be required to proceed in sequential order through the graduated steps of a technical assistance request (**TAR**), a technical assistance notice (**TAN**) and a technical capability notice (**TCN**) in dealings with a particular recipient in relation to a particular form of encryption where prior dealings of law enforcement agencies 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 of law enforcement agencies (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.

13. The power to invoke a requirement for a provider outside Australia of an electronic service that has no connection with Australia other than the possible unrelated fact that one or more end-users of the e-service are in Australia (see proposed sections 317C and 317D) – that is, where the encrypted communication may have no other relevant link to Australia, or to that or those end-users in Australia – is fundamentally different in nature and scope to a power to require a telecommunications carrier or carriage service provider operating within Australia to provide a capability to intercept a communication in transit or a stored communication on that provider's server. The Exposure Draft Bill would permit TANs and TCNs to be served on entities incorporated outside Australia in a number of ways, including by serving them on an address in Australia where that company 'conducts activities' (even though those activities may be unrelated to provision of the electronic service or the location of relevant end users). Agencies may therefore affect service of TANs and TCNs based on an insubstantial nexus.

14. The power potentially may be exercised against any provider of an electronic service anywhere in the world (that has at least one end-user in Australia), such as a financial services provider or a website operator accepting electronic payments. The weighting of the fundamental human right to privacy accordingly should be at least as high as for existing telecommunications interception powers and powers to view (access) content of unprotected communications. The Exposure Draft Bill should require the decision-maker to consider whether the interference in the fundamental human right to privacy is outweighed by the need to protect society from significant threats and to protect the personal safety of individuals. The Exposure Draft Bill permits TANs and TCNs to be issued based on the subjective view of individuals, without requiring an independent evaluation and authorisation by a judicial officer. 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 communication, issuance of a TAN or TCN should require authorisation by a judicial officer (judge or fulltime member of the Administrative Appeals Tribunal (**AAT**)).

15. The traditional main exceptions to the prohibition on interception broadly are:

    - enforcing the criminal law and laws imposing pecuniary penalties;
    - protecting the public revenue; and
    - safeguarding national security.

16. In the Exposure Draft Bill:

    - in addition to the traditional main exceptions, the purpose of 'assisting the enforcement of the criminal laws in force in a foreign country'[5] is included, which was relatively recently introduced into the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) pursuant to the *Cybercrime Legislation Amendment Act 2012* (Cth);
    - in the context of TARs only, the purpose relating to 'safeguarding national security' is broadened to include 'the interests of Australia's foreign relations or the interests of Australia's national economic well-being'; and[6]
    - in the context of TANs and TCNs, the four primary purposes (or relevant objectives as defined in the Telecommunications Act) is further expanded to include any matter that facilitates, or is ancillary or incidental to, primary purposes or relevant objectives, whichever is applicable.[7]

17. The Law Council submits that given the extensive powers already available to law enforcement authorities to access stored communications, metadata, and computer networks, it would be more reasonable and proportionate that the purposes for which

[5] See relevant objectives defined in s 317G(5)(b) of the Exposure Draft Bill with respect to requirements under TARs (per s 317G(2)); specified purposes for TANs under s 317L(2)(c)(ii); and relevant objectives defined in s 317T(3)(b) with respect to requirements for TCNs under s 317T(2).

[6] Compare proposed paragraph 317L(2)(c) of the Exposure Draft Bill for TANs: 'safeguarding national security'; proposed paragraph 317T(3)(d) for TCNs: 'safeguarding national security'; and proposed paragraph 317G(5)(d) for TARs: 'the interest of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being'.

[7] See proposed paragraph 317(L)(2)(d) of the Exposure Draft Bill for TANs and proposed subparagraphs 317T(2)(a)(ii) and 317T(2)(b)(ii) for TCNs.

the TARs, TCNs, and TANs can be given should be utilised only for matters of law enforcement involving serious criminal offences.[8]

18. If 'assistance to foreign law enforcement' is to remain as a basis for giving a TAR/TAN/TCN, the Law Council submits that 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 relevant decision-maker ought be required to 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). The Law Council also suggests that it may be appropriate for costs of compliance to be an additional matter for consideration by the decision-maker, particularly with respect to TAN/TCNs, where the mandatory aspects mean that Australian intelligence services may compel Australian service providers to undertake extensive and potentially resource-draining activities in response to assistance requests from foreign law enforcement agencies.

19. The rationale behind the third purpose, 'protecting the public revenue', has not been discussed in the commentary around the Exposure Draft Bill, and could potentially give the Australian Taxation Office (**ATO**), through cooperation with an interception agency, near-unlimited access to all encrypted communication on the basis that it might be evidence of a transaction giving rise to a tax liability. Although the purpose of 'protecting the public revenue' has been a part of the Telecommunications Act since its inception, it is unclear why such purpose should also be included in the Exposure Draft Bill given the greater business and human rights impact, substantial enlargement of interception agency powers and substantial expansion in range and geography of prospective recipients being proposed.

20. The Law Council suggests further that the purpose of 'safeguarding national security' has an extremely broad scope given that no actual laws need to be identified for it to apply. In the circumstances, where this appears to be a supplementary 'top up' power for law enforcement and will have a significant effect on the fundamental human right to privacy, the Law Council submits that this should be aligned with the current definition of serious offences in the TIA Act which would cover most critical matters of national security.

21. The Law Council has already noted that the Exposure Draft Bill would permit TARs and TCNs to be served on entities incorporated outside Australia in a number of ways, including by serving them on an address in Australia where that company 'conducts activities' (even though those activities may be unrelated to provision of the electronic service or the location of relevant end users). Agencies may therefore effect service of TANs and TCNs based on an insubstantial nexus. The recipient is nonetheless compelled to comply with the TAN or TCN notwithstanding the requirements of laws of foreign countries. Compliance by the recipient may compel businesses with only incidental nexus with Australia to take actions that violate the laws of other countries in which they have substantial operations and where they must take the relevant action to comply with the TAN or TCN. When those laws conflict with the lawful imperative of the TAN or TCN , the businesses would be left having to arbitrate between them or decide whose laws to violate, knowing that in doing so they might risk sanctions. That

[8] The definition of serious offences in section 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) is useful here, as it includes acts of terrorism, sabotage, espionage, foreign interference, and other serious criminal offences as well as offences which would prejudice national security. Alternatively, the concept often included in mutual assistance arrangements might be utilised, such as a criminal offence under a foreign law where there is a reasonably comparable offence under Australian law and where that reasonably comparable offence carries a potential penalty of imprisonment for a period exceeding seven years.

is an unreasonable position for these businesses to be placed in, and cause serious concerns of comity in operation of private international law. When Australian law and other laws applicable to that business conflict, the businesses would be left having to decide whose laws to violate, and which sanctions to risk. These foreign laws may be well accepted laws of countries that Australia otherwise accords significant favour. For example, compliance with this Bill could be deemed incompatible with various requirements of the GDPR (e.g., that data be processed safely and securely, or that a data controller clearly disclose to a data subject when their personal data will be disclosed to a third party). Failure on the part of a US company to follow US laws to protect electronic communications from unauthorised access might give rise to criminal and civil liability under the US Stored Communications Act. A business should not be put in this serious jeopardy. This also reinforces the need for TANs and TCNs to only be issued by a judicial officer, and only issued in aid of investigation or prosecution of a serious criminal offence.

22. The ability to challenge TANs and TCNs as issued is limited by the Exposure Draft Bill. In particular, the content of, and decision to issue, a Notice is not subject to administrative review. The Bill also excludes the application of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and therefore its 'order of review', and thus leaves designated communications providers with limited options to seek judicial relief for Notices that have already been issued. This is particularly inappropriate where the decision-maker is not a judicial officer. Further, to the extent any judicial review can be sought, it appears this would be retrospective, i.e. it could only be sought once the Notice has already been issued and complied with. Of course, once a notice is complied with, potential exposures have already occurred and the consequences may not be rectifiable, even if a court then finds the notice to have been illegal. The Law Council submits that it is inappropriate to limit the scope of judicial review in respect of such intrusive powers, and that they should be subject to a judicial process that explicitly provides for TANs and TCNs to be challenged before a judicial authority and set aside before compliance is required.

23. The Law Council submits that the Exposure Draft Bill may not take into account the realities of technology, in particular, the speed with which targeted criminals will shift platforms or adopt new technology.

**Recommendations**

- **Each interference in the fundamental human right to privacy should be considered and weighted against: any perceived imperative to protect society from significant threats and to protect the personal safety of individuals; and the expansion of purposes (or 'relevant objectives' as variously defined in the Exposure Draft Bill) which are used to carve out exclusions to the prohibition on access to communications.**
- **The legislation should expressly state that the power to request or require decryption (or an individual to facilitate opening up a password protected device) does not displace the need for an agency to obtain lawful authority to view the content of a communication or electronic record.**
- **The legislation should clearly identify the intended graduated operation of a TAR, a TAN and a TCN powers.**
- **As a primary recommendation, the Law Council recommends that the Exposure Draft 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 Exposure Draft Bill is designed to address.**

- **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). 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 also suggests that costs of compliance should be an additional matter for consideration by the decision-makers, particularly with respect to TAN/TCNs.**
- **The Exposure Draft Bill should require the decision-maker to consider whether the interference in the fundamental human right to privacy is outweighed by the need to protect society from significant threats and to protect the personal safety of individuals.**
- **The Law Council suggests further that proposed paragraph 317(L)(2)(d) of the Exposure Draft 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 Exposure Draft 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 communication, issue of a TAN or TCN should require authorisation by a judicial officer (judge or fulltime member of the AAT).**
- **A recipient of a notice that has its principal place of business outside Australia or that would require to take action to comply with the notice outside Australia should not be required to comply with a notice where to do so would cause the recipient to breach a mandatory requirement of a foreign law to which that entity is subject.**

# The scope of the Exposure Draft Bill as it relates to entities

24. The Law Council understands that the Exposure Draft Bill is intended to capture all types of entities which may have control over encrypted information of value to law enforcement.

25. The Explanatory Document to the Exposure Draft Bill states that the powers in the Bill 'cannot be used to impose data retention capability or interception capability obligations'. However, the language in the Bill does not prevent a TAN or TCN from requiring a designated communications provider that is not a carrier or carriage service provider to facilitate or instil a data retention or interception capability or to provide access to the content of a communication or electronic record in any circumstance where provision of that access requires a warrant or authorisation where the recipient is a carrier or carriage service provider. This outcome arises because only carriers and carriage service providers are subject to the TIA Act and the

Telecommunications Act and the instruments issued pursuant to that legislation, and accordingly subject to the important relevant carve-outs and requirements to protect personal privacy. In other words, the laws affecting carriers and carriage service providers contain protections and controls relating to the exercise and use of the powers and information collected from carriers and carriage service providers, but those protections and relevant controls do not extend to the important new and much larger group of providers of electronic services. The absence of these protections places a designated communications provider, who is not a carrier or carriage service provider, at a disadvantage as it may discourage users from trusting services they provide. In addition, there is nothing to prevent a TAN or TCN from requiring a service provider that is a regulated telecommunications provider in a foreign jurisdiction (but not Australia) from facilitating or installing interception.

26. The Law Council notes that the Exposure Draft Bill applies to 'eligible activities' of a 'designated communications provider', pursuant to proposed section 317C. These include the provision of a service 'ancillary or incidental to, the supply of a listed carriage service', the provision of 'an electronic service that has one or more end-users in Australia', the manufacturing and operation of a facility, and the manufacture of components used in a facility. The Law Council considers that many of these providers will have little or no control over encrypted information which will be of value to law enforcement, and it is unclear why they have been captured in the Exposure Draft Bill. This would make the Exposure Draft Bill a compliance concern for overseas companies operating in Australia, even if they have no control over encrypted communications.

**Recommendations**

- **The Exposure Draft Bill should be amended to ensure that protections of Australian telecommunications carriers and carriage service providers which 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 Law Council suggests that the entities to which the Exposure Draft Bill could apply should be limited to entities which have control over encrypted information and are able to access and decrypt it.**

# The scope of the Exposure Draft Bill as it relates to activities

27. The Law Council notes with agreement that:

- agencies must obtain a warrant or authorisation under the TIA Act, SDA or Crimes Act;
- there are requirements for practicability and technical feasibility;

- no systemic weaknesses can be built into products;[9] and
- some of the recommendations from the Law Council submission relating to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 have been adopted.[10]

28. However, the Law Council is concerned that:

- the Exposure Draft Bill can potentially require designated communications providers to undertake a wide range of activities unrelated to decrypting information, including installing, maintaining, testing or using software or equipment (proposed paragraph 317E(c)), assisting with the testing, modification, development or maintenance of a technology or capability (proposed paragraph 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));
- although TCNs cannot require a provider to build a new decryption capability, 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;
- the terms 'practicability' and 'technical feasibility' are not defined. The Law Council understands that any provider who believed a notice required them to undertake something unfeasible would need to seek judicial review; a potentially time-consuming and expensive process, particularly for a small business; and
- while the scope of notices is limited to core agency functions, these are very wide.[11]

**Recommendations**

- **The Bill should prohibit a Notice 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 Exposure Draft Bill be amended to limit the scope of application to companies with direct control and access to encrypted information.[12]**

[9] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 s 317ZG.
[10] Namely, that 'the agencies which can access telecommunications data must be exhaustively set out in the legislation' (Law Council of Australia, Submission No 126 to Parliamentary Joint Committee on Intelligence and Security *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. 20 January 2015, 4).
[11] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ss 317G(3) and 317T(3).
[12] 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

# Managing compliance costs

29. The Law Council considers that the advantages of the Exposure Draft Bill in relation to managing compliance costs include:

    - enforcement on a no profit/no loss principle; and
    - immunity from civil liability for cooperating providers.[13]

30. However, the Law Council is concerned:

    - there may be potentially unnecessary regulatory costs on providers. The Law Council notes that it can be burdensome for small businesses, in particular, with non-compliance fines of up to $10 million for companies and fines of up to $50,000 for individuals *per case,* where 'case' is not clearly defined*;*
    - agencies can issue TCNs to companies outside of Australia but within its 'nexus'. Agencies also require a warrant to undertake surveillance activities under the Exposure Draft Bill. These warrants have no application outside of Australia. The Law Council considers that it is unclear how this will operate; and
    - there should be considerations of the economic impact of the regime on small business holders. Where warrants or authorisations are issued to innocent holders of encrypted data, there is a risk that part of the investigative cost will be transferred to those holders. Where the holders are small businesses, the Law Council is concerned about the risk of government bodies requiring the holders of the data to utilise their own resources to make the data 'intelligible' to the relevant government body beyond merely de-encrypting the data.

**Recommendations**

**The Exposure Draft Bill 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 when the warrant giving the authority to issue the TCN does not apply.**
- **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.**

---

modification of, any of the characteristics of a service provided by the designated communications provider (proposed paragraph 317E(h)).

[13] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ss 317ZJ and 317G.

# Protection of privacy

31. The Law Council considers that one of the Exposure Draft Bill's primary advantages regarding protection of privacy is that it provides for unauthorised disclosure of information being punishable by up to five years' imprisonment.[14]

32. However, the Law Council understands that the 'public interest' test does not require decision-makers to have regard to privacy[15] when making a TAN or TCN.

33. A related issue is the exposure of recipients of warrants and authorisations to claims by parties the subject of the data sought by the warrant. Where data holders have contracted to protect such information, such as via the use of encryption, the Law Council is concerned that in complying with the warrant or authorisation, they may be exposing themselves to contractual claims. Most contracts allow carve outs for the provision of confidential information 'where required by law'. However, where there is an obligation to encrypt data and a warrant requires the recipient to de-encrypt such data, it is less clear that such steps would fall within such a contractual carve out.

34. The immunities for compliance with Notices are incomplete. The immunities would only be effective if the action is brought against a provider in Australia. Providers operating in jurisdictions outside of Australia are unlikely to be able to rely on the immunity in an action brought in a foreign jurisdiction, including an action for breach of laws in those jurisdictions that manifestly conflict with the requirement of a Notice. Additionally, the immunity would not act as an indemnity, and providers may still be exposed to liability for claims from third parties in a foreign country (e.g. for disclosure of confidential information or breach of a provider's contract with that third party). This leaves a provider having to attempt to overlay compliance with other foreign laws and commercial agreements in countries where they operate, and to bear the risk arising from that. This is not a reasonable position to create for providers, particularly where the nexus of their operations to Australia is weak.

**Recommendations**

- **The Law Council considers that the reasonable/proportionate test[16] should explicitly include a requirement to consider reasonable alternatives as may be available to the grant of the notice and specifically require the decision-maker to consider whether the interference in the fundamental human right to privacy is outweighed by the need to protect society from significant threats and to protect the personal safety of individuals.**
- **The scope of the immunity should be considered in light of potential contractual and other legal consequences to the recipients of warrants and authorisations regarding the parties to which any data the subject of the warrant relates.**

[14] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 s 317ZF.
[15] Ibid s 317ZK(2).
[16] Namely, that 'the decision-maker must be satisfied that requirements in a technical assistance notice and technical capability notice must be reasonable and proportionate and compliance with the notice is practicable and technically feasible'.

# Accountability/oversight

35. Regarding accountability and oversight under the Exposure Draft Bill, the Law Council notes:

    - the proposed safeguards that require warrants and strict threshold tests; and
    - only the Attorney-General or the head of an interception agency can issue a TCN.

36. However, the Law Council is concerned that:

    - the Exposure Draft Bill does not impose the same requirements for warrant or authorisation on a TAR, so there is less oversight compared to a TAN and a TCN;
    - annual reporting requirements and company transparency reports are arguably insufficient given the proposed scope of the Exposure Draft Bill; and
    - heads of interception agencies can delegate powers to Senior Executive Service employees.[17]

**Recommendations**

- **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.**
- **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.[18]**
- **The Law Council's previous recommendation that the Office of the Australian Information Commissioner has direct oversight to ensure the Australian Privacy Principles under the *Privacy Act 1988* (Cth) are complied with be adopted.[19]**

# Comparison with other jurisdictions

37. The Law Council is concerned that restrictions on encryption by other nations disproportionately affect the right to freedom of expression.

38. The Law Council notes that the United Kingdom's *Investigatory Powers Act 2016* (UK) (**the UK Act**) is broader in scope than the Exposure Draft Bill. The UK Act introduces a new system for the lawful interception and examination of information, authorisations for obtaining and retaining data, and new powers to issue notices to compel communications providers to do certain things, such as remove electronic protection by or on behalf of that operator from any communications or data, or disclose certain information.

[17] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ss 317ZP-317ZR.
[18] 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.
[19] Law Council of Australia, 'Policy Statement: Rule of Law Principles' (March 2011), 4.

39. In relation to the 'Assistance' aspect of the Exposure Draft Bill, the Law Council notes the following differences between the UK Act and the Exposure Draft Bill.

## Oversight

40. The Exposure Draft Bill has:

> *limited oversight and accountability structures and processes in place. The Director-General of Security, the chief officer of an interception agency and the Attorney-General can issue [technical capability] notices without judicial oversight. This differs from how it works in the UK, where a specific judicial oversight regime was established, in addition to the introduction of an Investigatory Powers Commission.*[20]

41. Under the Exposure Draft Bill, a TAN or TCN will 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 a range of laws is required.[21]

## Limitations

42. In the Exposure Draft Bill, the requirements imposed by a TCN must be reasonable and proportionate, and compliance must be practicable and technically feasible.[22] The UK Act specifically considers the cost to providers of complying with a notice:

> *the UK's Investigatory Powers Act authorises the UK Government to compel communications providers to remove 'electronic protection' applied to communications or data in its control. In requiring a person to remove such electronic protection, which would include encryption, the Government must in particular take into account the technical feasibility, and likely cost, of complying with those obligations*.[23]

## Preventing creation of 'back-doors'

43. The Exposure Draft Bill includes a provision that designated communications providers must not be required to implement or build a systemic weakness or systemic vulnerability into their systems.[24] The Law Council notes that it does not appear that such a provision exists in the UK Act, but commends this exception.

## Types of notices

44. The UK Act sets out two types of notices that compel assistance: national security notices and technical capability notices. National security notices require a telecommunications operator to take 'such specified steps as the Secretary of State

---

[20] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', *The Conversation* (online), 15 August 2018 <https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909)>; see also *Investigatory Powers Act 2016* (UK) ss 253(1) and s 254.

[21] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 s 317ZH.

[22] Ibid s 317V.

[23] Allens, 'Code Breakers – Australian Government Flags Forced Decryption Reforms', (https://www.allens.com.au/pubs/priv/pulse-1805/article-01.htm); see also *Investigatory Powers Act 2016* (UK) s 255(3).

[24] Exposure Draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 s 317ZG.

considers necessary in the interests of national security'[25] and technical capability notices impose on a relevant operator any obligations specified in the notice. This differs from the Exposure Draft Bill, which allows for technical capability notices to be issued to enforce domestic laws, assist the enforcement of the criminal laws of foreign countries, and in the broader interests of national security, or to protect the public revenue. These have been described as 'vague and unclear limits on these exceptional powers'.[26]

## Broad application

45. The Law Council understands that, in the UK Act, technical capability notices may be given to a 'relevant operation', meaning 'a postal operator, a telecommunications operator, or a person who is proposing to become a postal operator or telecommunications operator'.[27] In the Exposure Draft Bill, the term 'provider' is very broad and might include telecommunication companies, internet service providers, email providers, social media platforms and a range of other 'over-the-top' services. It also covers those who develop, supply or update software, and manufacture, supply, install or maintain data processing devices.[28]

46. The Law Council notes the following similarities between the UK Act and the Exposure Draft Bill in relation to the 'Assistance' aspect of the Exposure Draft Bill:

    - both the UK Act and the Exposure Draft Bill put the onus on telecommunication providers to give security agencies access to communications;[29] and
    - in both the UK Act and the Exposure Draft Bill, there are unclear outcomes for end-to-end encryption security. In Australia, 'providers will be required to develop new ways for law enforcement to collect information. As in the UK, it is not clear whether a provider will be able to offer true end-to-end encryption and still be able to comply with the notices'.[30]

47. Regarding the differences between the UK Act and the Exposure Draft Bill in relation to the 'Access' aspect of the Exposure Draft Bill, in the UK Act, there are safeguards in place for members of parliament, items subject to legal privilege, confidential journalism material and sources of journalistic information in relation to the issuing of warrants to intercept and examine information.[31] It does not appear that similar safeguards are contained in the Exposure Draft Bill.

48. While the Exposure Draft Bill does not concern data retention, the Law Council notes that recent legal challenge may lead to the UK having to amend the UK Act to the extent that 'it was inconsistent with EU law because access to retained data was not

[25] *Investigatory Powers Act 2016* (UK) s 252.
[26] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', *The Conversation* (online), 15 August 2018 <https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909)>.
[27] *Investigatory Powers Act 2016* (UK) s 253(3).
[28] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', *The Conversation* (online), 15 August 2018 <https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909)>.
[29] Ibid
[30] Ibid.
[31] *Investigatory Powers Act 2016* (UK) Part 2.

limited to the purpose of combating 'serious crime' and was not subject to prior review by a court or other independent body'.[32]

49. In considering the similarities and the differences between the Exposure Draft Bill and similar legislation found within the rest of the Five Eyes intelligence community, the Law Council notes the following:

- 'The enforcement of criminal laws in other countries may mean international requests for data will be funnelled through Australia as the 'weakest-link' of our Five eyes allies. This is because Australia has no enforceable human rights protections at the federal level';[33]
- in New Zealand, 'the *Telecommunications (Interception Capability and Security) Act* was introduced in 2013. It provides for the issuing to NZ surveillance agencies of warrants, under which they may require a telecommunications service to decrypt a telecommunication on its service if it has provided the encryption';[34] and
- in the United States, 'the Trump administration and FBI officials have publicly canvassed the possibility of cracking down on the use of encryption technology. This follows the 2016 legal battle between the Obama administration and tech giant Apple over whether Apple should be compelled to develop software allowing it to break into its own iPhone devices, in response to a terrorist attack in California. The FBI withdrew its request the day before the hearing of this dispute, claiming it had found a third party who was able to assist in unlocking the iPhone. Similarly to the situation in Australia, concerns in the US revolve around the inability to guarantee the security of decryption keys stored in a central location. This is why providers of encrypted communication services generally do not hold keys themselves. It is also unclear how the UK and NZ laws will work in circumstances where service providers are unable to decrypt, or have great difficulty in decrypting, communication'.[35]

**Recommendations**

- **The Law Council recommends that proposed paragraph 317V(b) of the Exposure Draft Bill be amended so that the Attorney-General must consider the likely cost of complying with a notice, as stated in section 255(3) of the UK Act.**
- **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 Exposure Draft Bill's potential negative impact to personal privacy for which individuals will have little recourse.**

[32] Ian Cobain, 'UK has six months to rewrite snooper's charter, high court rules', *The Guardian* (online), 28 April 2018 <https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules>.
[33] Monique Mann, 'The Devil is in the Detail of Government Bill to enable Access to Communications Data', *The Conversation* (online), 15 August 2018 <https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909)>.
[34] Allens, 'Code Breakers – Australian Government Flags Forced Decryption Reforms', (https://www.allens.com.au/pubs/priv/pulse-1805/article-01.htm).
[35] Ibid.

# Conclusion

50. There is significant value to public safety in allowing law enforcement agencies and authorities faster access to encrypted information where there are threats to national security, or in order to prevent the commission of serious criminal offences. However, the Law Council supports the guiding principle that the 'protection of privacy should continue to be a fundamental consideration in and the starting point for any legislation providing access to telecommunications for security and law enforcement purposes'.[36]

51. The recommendations above seek to balance the need for the protection of privacy with the overarching aims of the Exposure Draft Bill. They primarily revolve around limiting the scope and purpose of the Exposure Draft Bill so that individual freedoms are not unnecessarily and unintentionally encroached. Amending the Exposure Draft Bill in accordance with the Law Council's recommendations will assist in achieving such balance.

[36] Anthony Blunn, *Report of the Review of the Regulation of Access to Communications, Attorney-General's Department* (2005), 5. See also Law Council of Australia, Submission No 21 to the Parliamentary Joint Committee on Law Enforcement, *Inquiry on the Impact of New and Emerging ICT on Australian law enforcement agencies*, 6 February 2018, 7.