Law Council
OF AUSTRALIA

Office of the President

27 November 2018

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Mr Hastie

Law Council supplementary submission for the inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

1. Thank you for the opportunity for the Law Council to provide an additional written submission to the Parliamentary Joint Committee on Intelligence and Security's (**the Committee**) inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**the Bill**) following the Law Council's first appearance before the Committee on 19 October 2018.

2. During the Law Council's appearance at the 19 October 2018 hearing, Committee members asked the Law Council questions on notice relating to the meaning of the term 'electronic protection' and in relation to section 313 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**). Separately, on 20 November 2018 the Law Council was asked a question regarding the constitutionality of the powers in Schedule 1 of the Bill. This submission provides the Law Council's responses to those questions.

Meaning of electronic protection

3. During the 19 October 2018 hearing, the Hon Mark Dreyfus QC MP asked the following question on notice of the Law Council:

> *In a similar vein, does the Law Council think that the meaning of the term 'electronic protection', which is the term used throughout schedule 1, is clear?*

4. The term 'electronic protection' does not have specific legal meaning unless one is expressly drafted or created. Typically, reference is made to protection of electronic information and electronic communication.[1] In common usage, it might be reasonably suggested that 'electronic protection' is any form of protection of human intelligible information by an electronic barrier between a human and presentation of human intelligible information on a computing device (i.e. personal computer, tablet, smart

[1] See, e.g., *Directive 2009/136/EC of the European Parliament and of the Council on e-Privacy Directive Amendments* [2009] OJ L337/11 and *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC* [2017].

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

phone and other internet accessible device). The barrier may be between locally stored information on the device and remotely accessible services, including internet services, and databases accessible through use of a device. Those services may or may not be encrypted. Electronic protection may require entry of a password or passcode (including by requiring entry of a simple passcode into a device and more complex verification of identity for access to a particular application such as two factor verification for access to an online banking application; biometrics such as fingerprint, image and iris recognition; and/or use of an external secure access device such as a 'dongle'). A room or building may be electronically protected by requiring use of a swipe card or other means such as entry of a code: again, internet enabled verification of the swipe card or code manually entered by a human may be a feature of the electronic protection, but it is not a necessary feature (as codes may be locally stored).

5. By contrast, the term 'encryption' is well understood to mean:

> *… a process of transforming data through an algorithm into a format that can only be deciphered by an authorized individual. An encrypted data stream can only be decrypted with the correct 'key'*.[2]

6. Encryption is a particular form of electronic protection, where even if a service or data becomes available (for example, after passing through a form of electronic protection such as a password or pass code), the information then presented is not in human readable form. Accordingly, electronically protected information may or may not be encrypted, and encrypted information is subject to a form of electronic protection but may or may not be subject to requirement for human activity (such as entry of a password or pass code) to be presented to a human in readable form.

7. There is not sufficient information provided by the drafters of the Bill to understand the particular context in which electronic protection and encryption are respectively used in the Bill and whether the use of those terms is consistent with the above interpretation. The Law Council recommends that reference is generally made to 'encryption', as a term that is well understood in industry and the community. If need be, the term could be defined in a technologically neutral manner similar to the definition referenced above.

8. The Law Council also recommends that reference to 'systemic weaknesses' in section 317T, be replaced with more precise language that addresses any ongoing diminution in effectiveness, reliability and defensibility of security controls that may arise as a result of an intervention. The term 'systemic' does not have a reliably consistent meaning in this context the interpretation of that term by lawyers and information technologists may significantly conflict. The relevant factor should be that a weakness is introduced into a system (as that 'system' is constituted by a computing and data management environment, which may be the combination of a device, the operating system of that device, an application or program on a device and a service accessed through the use of that application or program) and the intervention is a cause of that weakness. In other words, the key criterion is that there is a new weakness in controls and safeguards as to access to information which is an ongoing or enduring weakness in controls and safeguards, which may or may not be a weakness of a particular system or sub-system relating to or affecting that device.

[2] Bloomberg Law BNA, *Privacy* <https://www.bloomberglaw.com/product/privacy/search/results/2960e5356c1fabfdcd7c50701fa7a61c>.

9. As the Committee appreciates, the term 'systems' and 'systemic' is commonly used in various technology standards[3] and may be interpreted as requiring that for a weakness to be systemic, that weakness must affect the working of a particular security system. This makes it a very vague and potentially a high standard to meet before planned intervention can be said to be inappropriate in a given scenario.

Section 313 of the Telecommunications Act

10. During the 19 October 2018 hearing, the Hon Julian Leaser MP asked the following question on notice of the Law Council:

> *I echo what everybody else has said about the submission. Thank you very much. I want you to take a matter on notice because we don't have time for you to answer it here. I'm interested in the operation of section 313 of the act and to what extent this bill is an improvement. What are some of the shortcomings of section 313 that this bill has addressed and that you wouldn't want to see replicated? I wondered if you might give some consideration to that in your further submission.*

11. Unfortunately, there is no simple answer to this question, as the intended interaction between the provisions of this Bill and ongoing operation of section 313 is difficult to understand, interpret and apply. The provisions which are most problematic are subsections 317ZH(1) and (2), which requires artificial 'assumptions' to be made when interpreting other statutory provisions, including section 313, as applying to provisions of this Bill. This is of particular concern, as subsections 317ZH(1) and (2) are fundamental provisions to whether access to the context of a communication through mandatory decryption is not required in any circumstance where access to unencrypted (human readable) content would require a warrant or authorisation.

12. In any event, the Bill authorises voluntary acts taken upon request, so many recipients of 'requests' from a law enforcement agency may simply comply with the request, without requiring compulsion under subsections 313(3) or 313(4).

13. Where a (mandatory) notice is issued, if the notice is issued to a carriage service provider (i.e. a provider of a messaging service that carries messages from point A to point B, such as WhatsApp, etc.) the effect of proposed section 317ZH appears intended to be that a technical assistance notice or a technical capability notice 'has no effect to the extent that' a warrant or authorisation (including a journalist information warrant under Division 4C of the *Telecommunications (Interception and Access) Act 1979* (Cth) – **TIA Act** – as amended by the mandatory metadata retention laws) would be required for a carrier or carriage service provider to be obliged pursuant to section 313 of the Telecommunications Act to give help to a law enforcement agency. However, one reading of paragraph 317ZH(2)(b) is that it would extend the operation of subsection 313(3) and (4) to include anyone within the large new class of designated communications providers that are not also carriers or carriage service providers, with the effect that the mandatory operation of subsections 313(3) and (4) is extended to these other providers. It is then not clear whether a separate warrant or authorisation is required before a designated communications provider is obliged to provide access to content of communications through bypassing forms of electronic protection.

[3] See, e.g., Marianne Swanson and Barbara Guttman, 'Generally Accepted Principles and Practices for Securing Information Technology Systems' (Special Publication, National Institute of Standards and Technology, September 1996) 25.

14. Further, the present provisions of the TIA Act do not exclude or limit operation of other and inconsistent laws, only limiting its own operation in relation to communications to ensure that access to content of communications under that Act requires a warrant. There may be a possibility therefore for an 'authorisation' under state or territory legislation for access to particular information to, of its own force, include authorisation (that is, not a warrant) for access to content of a communication. In this circumstance that authorisation is effective to engage operation of subsections 313(3) and (4), such that a warrant is required and a notice under the new provisions may operate to require breaking electronic protection to allow access to the content of a communication, without any warrant. That is, section 317ZH does not clearly evidence an intention to override inconsistent state or territory laws.

15. The above concerns are heightened by the breadth of potential operation of these provisions. As our previous submission noted, these provisions extended beyond detection and investigation of terrorism and other serious criminal offences under Australian law, to include any detection and investigation of any suspected criminal offence and enforcement of laws for recovery of pecuniary penalties. The key concern is the breadth and scope of the powers granted under this section, especially when considered in the context of the breadth of other provisions as noted previously. For example, the scope of the offences[4] and variety of providers in scope. This concern could be in part addressed by, expressly limiting the scope of the assistance required to support the warrant as granted on the terms as expressly granted and by requiring authorisation by a Judge or an Administrative Appeals Tribunal member as in the case of surveillance device warrants made under the *Surveillance Devoices Act 2004* (Cth). In addition, from a privacy perspective, the decision maker should be required (amongst other matters) to expressly consider the privacy impacts on affected individuals or groups of individuals and whether the proposed intervention (if any) is proportionate in the circumstances.

Constitutionality of Schedule 1 relating to 'designated service provider' and non constitutional corporations

16. The Law Council understands that the Committee asked the Department of Home Affairs a question regarding the constitutionality of the powers in Schedule 1 of the Bill and received the following response.

> ***Question from the Committee:*** The definition of 'designated service provider' extends to individuals and entities that are not constitutional corporations. Moreover, a provider may be compelled to do an 'act or thing' in relation to the enforcement of any criminal law or any law imposing a pecuniary penalty (not just laws with a federal aspect). Has the Department sought legal advice on whether the laws proposed in Schedule 1 are constitutional? If not, why not? If so, what did that advice say and would the Department be prepared to publish that advice in full?
>
> ***Department response:*** Yes, the Department did seek legal advice on the laws proposed in Schedule 1 and was advised that they were constitutional. Accordingly, the Department is satisfied with the constitutionality of the measures. Consistent with standard practice, the Department will not disclose legally privileged advice beyond the necessary Government stakeholders.

[4] Including protecting public revenue and services provided by third parties.

17. This question was prompted, in part, by the existence of proposed section 317ZT which provides for an alternative constitutional basis for the provisions in Schedule 1.

18. In advance of the Law Council's second appearance before the Committee in relation to the Bill on 30 November 2018, the Committee has indicated that it would be grateful if the Law Council could provide its view on whether the laws proposed in Schedule 1 are constitutional to the extent that a reference to a 'designated communications provider' in Schedule 1 includes a reference to an individual or entity that is not a constitutional corporation (noting also that a 'designated communications provider' does not have to be a telecommunications provider or carriage service but may be – for example – a natural person who merely operates or supplies components to 'a facility').

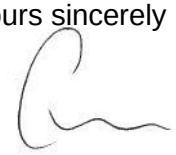
19. In addition to partial reliance on the corporations power in paragraph 51(xx) of the Constitution, it appears that the definition of a 'designated communications provider' primarily relies upon the 'postal, telegraphic, telephonic, and other like services' power in paragraph 51(v). To the extent that such bodies or persons as are defined as 'designated communications providers' and are engaged in matters concerning telecommunications or electronic communications, or their actions fall within the incidental aspect of such a power, they will be covered by a constitutional head of power. This should pick up most of the categories in the definition (although there will always be uncertainty as to how far the incidental power goes and how remote the connection to telecommunications can become while still being covered by the head of power). There may also be reliance on the external affairs power in paragraph 51(xxix) in relation to matters or things that take place outside of Australia, such as those concerning the actions of foreign manufacturers or telecommunications service providers.

20. In addition, there may be the possibility for the application of a patchwork of other Constitutional powers to cover any gaps, including the interstate and overseas trade and commerce power in paragraph 51(i), the territories power in section 122, the defence power in paragraph 51(vi) regarding national security issues such as terrorism and defence issues, and the nationhood power sourced from the combination of sections 61 and s 51(xxxix) of the Constitution with regard to the protection of the nation and the functions of the Commonwealth. Further, to the extent that the law concerns the facilitation of the enforcement of a valid Commonwealth criminal law, it may also fall within the incidental power with respect to the head of power used to enact that law.

I trust the above additional written submissions are of assistance to the Committee in its deliberations.

Please contact Natasha Molt, Director of Policy ((02) 6246 3754 or natasha.molt@lawcouncil.asn.au) in the first instance, if you require further information or clarification.

Yours sincerely



Morry Bailes
President