Law Council
OF AUSTRALIA

Office of the President

10 March 2020

Dr James Renwick SC
Independent National Security Legislation Monitor
PO Box 6500
CANBERRA ACT 2600

By email: INSLM@inslm.gov.au

Dear Dr Renwick

Supplementary Submission: Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)

Thank you for the opportunity for Law Council representatives to appear at the Independent National Security Legislation Monitor's (**INLSM**) public hearing on 21 February 2020 as part of the review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**).

During the course of the Law Council's appearance, the Law Council took two questions on notice. This supplementary submission provides a response to those questions.

Assessment under 317ZG

Current test in the TOLA Act

The first question relates to section 317ZG of the *Telecommunications Act 1997* (Cth). Subsection 317ZG(1) provides that a Technical Assistance Request (**TAR**), Technical Assistance Notice (**TAN**) or Technical Capability Notice (**TCN**) must not have the effect of:

a) requesting or requiring a designated communication provider (**DCP**) to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection; or
b) preventing a DCP from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.

Subsections 317ZG(4A)-(4C) state:

> *In a case where a weakness [or vulnerability] is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness [or vulnerability] into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.*
>
> …

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

> *For the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.*

Proposed reform by the Repairing Assistance and Access Bill 2019

The Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 (**Repairing Assistance and Access Bill**), currently in the Senate, seeks to amend section 317ZG.[1] At the hearing, you asked the Law Council for its view on proposed section 317ZG in the Repairing Assistance and Access Bill and, specifically, subsection 317ZG(4), which states:

> *The reference in paragraph (1)(a) to implement or build a systemic weakness, or a systemic vulnerability, includes a reference to any act or thing that would or may create a material risk that otherwise secure information would or may in the future be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.*

The Law Council agrees with your observations in your opening statement that proposed section 317ZG in the Repairing Assistance and Access Bill helpfully focuses on prohibited effects. The proposed provision makes clear that it seeks to protect effects which would not only unnecessarily compromise the privacy of customers, but also risk compromising the security of a DCP's product, as well as that of other users of the DCP's product (or of apps, products, systems and databases) that are, or may be, reasonably anticipated to be interworked with the DCP's product. The current words 'security of any information held by any other person' are not sufficiently clear that this information may reside outside the DCP's product and that the reference to 'any other person' is not limited to persons directly using the DCP's product.[2]

The Law Council has expressed support for the inclusion of concepts such 'material risk', 'otherwise secure information' and 'unauthorised third party' within section 317ZG and their proposed definitions.[3]

Regarding the definition of 'otherwise secure information', the Law Council has noted that further clarity should be provided through the express inclusion that 'otherwise secure information' is information that is directly or indirectly, of, about or relating to, any person who is not the subject of a TAR, TAN or TCN.[4]

At the public hearing, you queried whether the Law Council has considered the threshold that is proposed in subsection 317ZG(4) of 'would or may in the future'. The Law Council understands that your concern pertains to the potential of this threshold to create an unattainable standard because it may be that such a risk can never be ruled out.[5]

---

[1] Telecommunications Amendment (Repairing Assistance and Access) Bill 2019 cl 5.
[2] Independent National Security Legislation Monitor, *Opening Statement* (Public Hearing, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (Cth), 21 February 2020) 11 [36].
[3] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (23 January 2019) 31 [62]-[65].
[4] Ibid [65].
[5] Independent National Security Legislation Monitor, *Opening Statement* (Public Hearing, Review of the *Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018* (Cth), 21 February 2020) 8 [36].

The Law Council notes that some other legislated frameworks are based on the test of likelihood, such as in the misleading and deceptive conduct provisions within the Australian Consumer Law,[6] as does the definition of an 'eligible data breach' under the notifiable data breach scheme in the *Privacy Act 1988* (Cth) (**Privacy Act**).[7] Importantly, both regimes also focus on the impact on individuals.

However, the Law Council submits that alternatives to 'would or may in the future', such as 'will, or is likely to', in their context would be read as introducing a standard of certainty as to a futurity that is unreasonably high. Both terms 'would' or 'may' express a sense of possibility, as opposed to probability. The Law Council understands that the standard needs to be more than a mere possibility, and that setting a standard as to any futurity in relation to levels of information security is problematic.

The threshold of 'may' is, on balance, more appropriate because the term 'would' appears to have the same issue as to level of certainty as 'will', and arguably has the same meaning as 'will' but is less grammatically accepted usage. Additionally, it can be used to 'refer to a situation that you can imagine happening',[8] or in exclusion clauses, for example, to 'limit or exclude the liability of a party which would otherwise arise as a result of a breach by that party of his primary obligations to perform the contract in accordance with its terms'.[9] While 'may' can similarly be used to express possibility, it also expresses a permission to do something. This makes it marginally more relevant in this legislative context as these provisions focus on granting rights and creating obligations.

The words 'may create a material risk' could be said to be too broad and encompassing a mere possibility. The Law Council suggests that 'may be reasonably anticipated to create a material risk', or, less desirably, 'may be reasonably likely to create a material risk', is a more superior formulation. The Law Council reiterates the importance of ensuring that the information security thereby should be not only of a DCP's product and should include information security of apps, products, systems and databases that are, or may be, reasonably anticipated to be interworked with the DCP's product.

Law Council's proposed revisions to section 317ZG

The Law Council submits that an assessment of whether an industry assistance notice has the effect of weakening an electronic protection within a system requires consideration of whether:

(a) the action that is authorised by the notice creates or expands any ability of an agency or of a third party, whether or not authorised, to render into human intelligible form, any encrypted content of communications, or any encrypted information about communications, passing over a particular system or service, other than in the specific instance expressly addressed in and authorised by the notice;

(b) the action that is authorised by the notice creates or expands pathways or means through any other system or service by which agency or of a third party, whether or not authorised, may render into human intelligible form, any encrypted content of communications, or any encrypted information about communications, passing over a particular system or service, other than in the specific instance and the particular system or service as expressly addressed in and authorised by the notice; and

[6] *Competition and Consumer Act 2010* (Cth) sch 2, s 18.
[7] *Privacy Act 1988* (Cth) s 26WE.
[8] Cambridge Dictionary (online at 6 March 2020) 'would' (def 2) <https://dictionary.cambridge.org/dictionary/english/would>.
[9] Greig and Davis, *The Law of Contract* (Law Book Co, 1987) 597.

(c) whether any consequences of the action that is authorised by the notice is of the nature of introduction of an ongoing vulnerability or weakness of any service or system that is not readily ascertainable on the face of the notice, not being consequences only for the instance expressly addressed in and authorised by the notice.

The Law Council recommends that the assessment also requires consideration of risk factors that go to the nature of the information and activities as risk presented to individuals, specifically, other individuals who are not the subject of the investigation or interest, but rather are members of the community who may be impacted by activities authorised by the notice in question. To this end, the Law Council proposes that the assessment is to be made having regard to:

(a) the type of information typically processed by the agency or third party, the subject of the notice and the likely impact on an individual or individuals if that information was the subject of accidental or unlawful destruction, deletion, loss, alteration, unauthorised disclosure of or access to or storage of such information, for example;
   i. biometric information data;
   ii. health information;[10]
   iii. sensitive information;[11]
   iv. government identifiers;

(b) the type of service typically provided by the agency or third party, the subject of the notice and obligations that agency or third party has to protect the confidentiality and privacy of the information it holds, including matters such as whether the agency or third party the subject of the notice:
   i. provides a health service as defined and regulated by law;[12]
   ii. provides financial services as defined and regulated by law;[13]
   iii. uses, discloses or otherwise holds or processes sensitive information, biometric information, health information or information containing government identifiers or derived from or related to such identifiers;
   iv. offers goods or services to data subjects in the European Union or the European Economic Area (**EEA**) or monitors their behaviour as far as the behaviour takes place within the European Union or the EEA or is otherwise governed by other privacy and data protection laws such as the General Data Protection Regulation;[14]

(c) what obligation, if any, the agency or third party the subject of the notice has under Part IIIC of the Privacy Act, dealing with notification of eligible data breaches, or similar breach notification obligations applicable to personal information that apply to the agency or third party the subject of the notice; and

(d) what obligation, if any, the agency or third party the subject of the notice has under the relevant provisions dealing with cybersecurity risk or breaches or similar breach

[10] See *Privacy Act 1988* (Cth) s 6FA.
[11] See ibid s 6, definition of 'sensitive information'.
[12] See ibid s 6FB.
[13] See *Corporations Act 2001* (Cth); *Banking Act 1959* (Cth)
[14] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 art 3(2).

notification obligations applicable to data and information systems that apply to the agency or third party the subject of the notice.[15]

Appropriately targeted weaknesses and vulnerabilities

The second question related to actions of law enforcement which have legitimate operational objectives, but result in the creation or introduction of a compromise within a system. The Law Council was asked whether it considers that industry assistance notices can be used in a way so that weaknesses or vulnerabilities are sufficiently targeted to their purpose of investigating a suspect, and how such targeting could be achieved.

At the public hearing, reference was made to the powers of law enforcement agencies to request the creation of identity documents, such as false credit cards, for assumed identities in accordance with Division 3 of Part 1AC of the *Crimes Act 1914* (Cth) (**Crimes Act**). The Law Council understands the basis for the comparison was to contend that although the use of false identity documents by an 'assumed identity' for law enforcement purposes introduces a weakness into the integrity of Australia's identification document framework, this is necessary and proportionate to the legitimate operational objective.

The Law Council recognises that in some circumstances, it is legitimate for law enforcement agencies to introduce weaknesses or exploit vulnerabilities. However, as noted by Law Council representatives at the public hearing, the concern relating to weaknesses and vulnerabilities in the digital context is that they are more difficult to confine to the purpose of their introduction. Their potential for far-reaching and more permanent impacts calls into question how necessary and proportionate this measure is to legitimate operational objectives.

The Law Council does not consider that compromises to digital systems as a result of compliance with industry assistance notices can be targeted to the same extent as compromises introduced to offline systems through the exercise of existing offline investigatory powers, such as those found in Part 1AC of the Crimes Act. There are key distinctions between online and office system compromises.

The Law Council considers that it is easier to identify the veracity and authenticity of false documents used by assumed identities than it is to identify, and understand the implications of, a weakness that may introduced into a component, product or service. The Law Council notes that the Crimes Act contains provisions relating to the cancellation of evidence of an assumed identity.[16] However, it is not so easy to effectively 'cancel' the changes or modifications that were made to digital security standards in order to comply with either a TAR, TAN or a TCN. While DCPs are not prevented from 'patching' weaknesses or vulnerabilities,[17] it is unclear to what extent DCPs can 'patch' the weaknesses or vulnerabilities they were asked or required to implement through an industry assistance notice. This is compounded by the fact that weaknesses or vulnerabilities which are introduced into components could unknowingly, to both DCPs and agencies, infect devices or facilities in which the components are later installed.[18]

Under the Crimes Act, there are numerous safeguards which seek to ensure that the issuance of, for example, fake credit cards, and the related implications come most directly

[15] See Australian Prudential Regulation Authority, *Prudential Standard CPS 234 – Information Security* (July 2019) cls 35-6.
[16] *Crimes Act 1995* (Cth) s 15KL.
[17] *Telecommunications Act 1997* (Cth) s 317ZG(1)(b).
[18] Component manufacturers and component suppliers are included as designated communications providers: ibid s 317C item 6.

to bear on the suspect of the criminal investigation. For example, once the chief officer of a law enforcement agency requests the person to return any evidence of the assumed identity acquired under the authority, the person must comply with this request or the person is committing an offence pursuant to subsection 15KM(3) of the Crimes Act.[19] There are also safeguards which aim to ensure that the assumed identity, or evidence of one, is only used in accordance with the authority granted as to the use of the assumed identity.[20]

In summary, the Law Council considers that the potential implications of systemic weaknesses or vulnerabilities that may be introduced in the course of compliance with a TAR, TAN or TCN are not as easy to identify, target and regulate as the compromise that is inserted into Australia's identity verification system through the creation of an identity document for an assumed identity.

Thank you again for the opportunity to appear at the public hearing and provide this supplementary submission. Please contact Dr Natasha Molt, Director of Policy, on (02) 6246 3754 or at natasha.molt@lawcouncil.asn.au in the first instance, if you require further information or clarification.

Yours sincerely

Pauline Wright
President

[19] *Crimes Act 1914* (Cth) s 15KL.
[20] Ibid s 15LB.