Submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Law Council of Australia
Contact details *(one or all of the following: postal address, email address or phone number)*	Dr Natasha Molt Senior Policy Lawyer 02 6246 3754 natasha.molt@lawcouncil.asn.au

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically. The following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

Hardcopy submissions received by mail will still be considered, however they will not be published on the website.

Confidentiality

Submissions received may be published on the Attorney-General's Department webpage, except where requests have been made to keep them confidential or where they relate to particular cases or personal information.

Would you prefer this submission to remain confidential? NO

18 January 2015

Law Council
OF AUSTRALIA

Mr Andrew Rice
Assistant Secretary
Cyber and Identity Security Policy Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

By email: telco.security@ag.gov.au

Dear Mr Rice

Telecommunications Sector Security Reforms

1. Thank you for the opportunity to provide a submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015 (the Bill, also referred to as Telecommunications Sector Security Reform (TSSR)).

2. The Law Council acknowledges the importance of protecting telecommunications infrastructure and the information transmitted across it from espionage, sabotage and foreign interference. For this reason, the Law Council supports measures that ensure that Australia's networks and communications infrastructure are resistant to unauthorised external attack, particularly in light of the introduction of the data retention regime.

3. The Law Council is, however, concerned that aspects of the proposed TSSR are inconsistent with the rule of law on the basis that they are not both readily known and available, and certain and clear.[1] Privacy considerations raised by the Office of the Australian Information Commissioner (OAIC) also only appear to have been partly addressed by the current draft Bill. In that regard, the comments below are primarily aimed at ensuring the new security obligations on carriers and carriage service providers (C/CSPs) are certain and clear and that the measures are consistent with obligations under the *Privacy Act 1988* (Cth) (Privacy Act).

4. This submission does not focus on assessing arguments put forward by industry that the proposed regime has not been demonstrated to be necessary and whether alternative arrangements (such as best practice guidelines and suitable fora for information exchange) may be a more effective and responsive way to deal with cyber threats. The Law Council encourages the Attorney-General's Department to continue consultation with industry on such issues.

<u>Uncertain threshold remains for exercise of discretionary powers</u>

5. Section 315A of the Bill would (like current subsection 581(3) of the *Telecommunications Act 1997* (Cth) (Telecommunications Act)) grant the Attorney-General a broad power to give a C/CSP a written direction not to use or supply, or to cease using or supplying, the carriage service or the carriage services if he or she considers it is prejudicial to security. Section 315B would also grant the Attorney-General a broad power to give a carrier, carriage service provider or carriage service intermediary a written direction requiring the

[1] Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011, Principle 1, 2.

carrier, provider or intermediary to do, or to refrain from doing, a specified act or thing within the period specified in the direction. The Attorney-General must be satisfied that there is a *risk* of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities that would be prejudicial to security.

6. The threshold for the exercise of the directions powers has been increased by for example requiring in subsections 315A(3) and 315B(4) of the Bill an adverse security assessment to be furnished by ASIO.

7. An adverse security assessment is defined in section 35 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) and means a security assessment in respect of a person (including a company) that contains:

   (a) any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and

   (b) a recommendation that prescribed administrative action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.[2]

8. The issuing of an adverse security assessment is not required to be based on conventional standards of proof such as a 'balance of probabilities' test. The specific criteria by which ASIO make their assessments are also largely unknown (beyond the facts for example that it must relate to ASIO's functions and the definition of security in section 4 of the ASIO Act), making it uncertain as to when a cyber risk or threat will be considered to be of a sufficient level of seriousness to warrant the issuing of a direction by the Attorney-General.

9. For example, it is unclear whether a risk or prejudice to security must be substantial, likely, imminent or of severe potential impact before an adverse security assessment is issued. While merits review of ASIO's adverse security assessments would be available, this will not necessarily indicate the criteria used in the issuance of a security assessment.

10. Any process that may result in substantial impacts on providers and potentially the services provided to consumers must be, to the extent possible, transparent. The threshold for the exercise of the directions powers should only be permitted where there is a sufficient level of risk to security to justify the exercise of the powers. This could be achieved, for example, by amending subsection 315B(1) to require that the Attorney-General is satisfied that there is a substantial and imminent risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities that would be prejudicial to security.

Definition of 'prejudicial to security'

11. 'Security' is broadly defined in section 4 of the ASIO Act to include the protection of the Commonwealth, states, territories and the people of Australia from espionage, sabotage, attacks on Australia's defence system, and acts of foreign interference. It also includes the protection of Australia's territorial and border integrity from serious threats and carrying out of Australia's responsibilities to any foreign country in relation to protecting Australia's territorial and border integrity from serious threats.

12. The draft Explanatory Memorandum to the Bill notes that:

   'Prejudicial to security' is intended to have the same meaning as the term 'activities prejudicial to security' which is set out in the Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence). The term is defined to mean activities that are relevant to security and which can reasonably be considered capable of causing damage or harm to

[2] Section 35 of the *Australian Security and Intelligence Organisation Act 1979* (Cth).

Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities.[3]

13. However, the rule of law requires that the law must be both readily known and available, and certain and clear.[4] This requires that key terms should be defined.[5] To ensure that the Attorney-General's directions powers can only be exercised in the circumstances intended by the Explanatory Memorandum, the term 'prejudicial to security' should be defined in the legislation itself. This would also ensure that the term 'prejudicial to security' could not be later redefined without adequate Parliamentary scrutiny.

Over-the-top (OTT) services

14. The TSSR appears to apply to Australian based C/CSPs and carriage service intermediaries that supply OTT services. They do not apply to international OTT services or internationally based C/CSPs that provide OTT services. It is not apparent as to how the level of risk will be calculated in determining whether Australian based C/CSPs have maintained their security obligations under the proposed TSSR when they supply OTT services. The security obligations should relate to any additional likely level of security risk with the supply of OTT services when compared with the level of risk that applies where the service is obtained directly from the OTT service.

Carriage service intermediary

15. Existing section 7 of the Telecommunications Act defines 'carriage service intermediary' to mean a person who is a carriage service provider under subsection 87(5) of the Act. Given this, it is not clear why it is proposed to create separate obligations in subsection 313(2A) for carriage service intermediaries and in subsection 313(1A) for C/CSPs to protect telecommunications networks and facilities from unauthorised interference or access for the purposes of security. The Explanatory Memorandum should clarify why separate obligations are considered necessary or desirable or the Bill should be amended to remove the separate obligations.

16. Further, section 87 of the Telecommunications Act generally defines intermediaries as a person who 'arranges, or proposes to arrange, for the supply of a listed carriage service by a carriage service provider to a third person'. Under this definition it therefore appears that an intermediary may not own or manage networks or facilities. This would appear to make it very difficult or impossible for intermediaries to maintain competent supervision and effective control over networks and facilities. If the separate obligations are to be maintained, the scope of the obligation on carriage service intermediaries needs to be amended in subsection 313(2B) to recognise that intermediaries as defined in sections 7 and 87 of the Telecommunications Act do not necessarily have effective control over, telecommunications networks and facilities.

Definition of 'facility'

17. The definition of 'facility' in section 7 of the Telecommunications Act broadly includes 'any… equipment, apparatus… or thing used, or for use, in or in connection with a telecommunications network'. This would appear to capture cloud computing and cloud storage options implemented by C/CSPs. It is unclear how C/CSPs will be able to effectively maintain their security obligations in this context. The Law Council suggests the Attorney-General's Department consult with industry on the adequacy of this definition for the purposes of the TSSR.

---

[3] Explanatory Memorandum to the Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015, 14.
[4] Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011, Principle 1, 2.
[5] Ibid.

Notification of changes to telecommunications services or telecommunications systems

18. Proposed section 314A of the draft Bill provides that C/CSPs must notify the Communications Access Co-ordinator (CAC), in writing, if they become aware that the implementation of a change that is proposed to a telecommunications service or a telecommunications system is likely to have a material adverse effect on the capacity of the carrier or provider to comply with its obligations under subsection 313(1A) or (2A). The draft Bill then lists several kinds of changes that *may* give rise to an assessment by the C/CSP that it would be likely to have a material adverse effect on their security obligations. This appears appropriate as C/CSPs are well-placed through their practices and processes to identify particular risks associated with proposed changes.

19. However, the Explanatory Memorandum does not appear to be consistent with the draft Bill on this issue. It states that 'new section 314A of the Telecommunications Act outlines the types of changes in arrangements that should be notified to the CAC, which include but are not limited to: (….).' and then lists the kinds of changes.[6] The Explanatory Memorandum should be amended to reflect the revised Exposure Draft Bill.

Retrofitting systems to comply with security obligations

20. The draft Guidelines state with respect to the security obligations in section 313 that C/CSPs 'are not expected to retrofit all systems on commencement of this security obligation, except in very rare cases…'.[7] This intention, however, is not binding as it is not reproduced in the draft legislation. Given the severe impact that a requirement to retrofit all systems may have on C/CSPs, this intention should be reflected in the legislation to ensure it operates as intended.

Privacy considerations

21. The Law Council notes that a number of the OAIC's recommendations to the initial Exposure Draft Bill do not appear to have been addressed by the latest Exposure Draft Bill. The Law Council submits that the privacy concerns raised by the OAIC should be addressed in consultation with the OAIC and industry groups.

Requirement for C/CSPs to 'do their best'

22. For example, it is not clear on the face of the legislation that the obligations proposed by the Bill are additional and separate obligations or are consistent with thresholds in Australian Privacy Principle (APP) 11.1 in the Privacy Act and the new obligation under section 187 of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).[8] The Explanatory Memorandum notes that the obligation which is framed in terms of the C/CSP doing 'its best' requires C/CSPs to take all *reasonable steps* to prevent unauthorised access and interference for the purpose of protecting the confidentiality of information and the availability and integrity of networks.[9] Nonetheless, it is not clear that an obligation on a C/CSP to do 'its best' is the same as a requirement to take such steps as are reasonable in the circumstances which applies under APP 11.1, or whether the threshold is higher or lower.

Information-gathering powers

[6] Explanatory Memorandum to the Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015, [19].
[7] Draft Telecommunications Sector Security Guidelines, November 2015, 25.
[8] Office of the Australian Information Commissioner, *Submission to the Attorney-General's Department on the Telecommunications Sector Security Reforms*, August 2015, 3-5.
[9] Explanatory Memorandum to the Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015, 22.

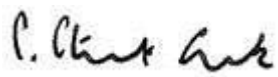
23. Sections 315C-215H of the Bill would establish new information-gathering powers for the Secretary of the Attorney-General's Department. The Secretary would be empowered to compel information from C/CSPs where the privilege against self-incrimination would not apply.[10] Information collected under subsection 315C(2) may be shared where it is for the purpose of either making the assessment of a C/CSP's compliance with their obligations, or for security purposes. While the information sharing may take place between government agencies, which are covered by the Privacy Act or a similar privacy regime, the OAIC recommended that to:

> *… protect the privacy of any affected individuals in the event that personal information is disclosed under s 315C(2)… the Bill should require that the entity to which the information is disclosed:*
>
> - *only use that information for the purposes in s 315H(1); and*
> - *not make any secondary disclosures of that information*.[11]

24. The action officer for this matter is Dr Natasha Molt, Senior Policy Lawyer (02 6246 3754 or natasha.molt@lawcouncil.asn.au).

25. Thank you again for the opportunity to provide these observations.

Yours sincerely



S. Stuart Clark AM
PRESIDENT
president@lawcouncil.asn.au

[10] A use and derivative use immunity would apply to certain proceedings.
[11] Office of the Australian Information Commissioner, *Submission to the Attorney-General's Department on the Telecommunications Sector Security Reforms*, August 2015, 8.

Attachment A: Profile of 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 2015 Executive as at 1 July 2015 are:

- Mr S. Stuart Clark AM, President
- Ms Fiona McLeod SC, President-Elect
- Mr Morry Bailes, Treasurer
- Mr Arthur Moses SC, Executive Member
- Mr Konrad de Kerloy, Executive Member
- Mr Michael Fitzgerald, Executive Member

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