Law Council
OF AUSTRALIA

Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)

Parliamentary Joint Committee on Intelligence and Security

16 July 2019

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 **3**
Acknowledgement **4**
Introduction **5**
Reporting by the Commonwealth Ombudsman **6**
Interaction with foreign laws **7**
Interaction with the United States CLOUD Act 7
Interaction with the laws of the European Union 10

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 2019 Executive as at 28 June 2019 are:

- Mr Arthur Moses SC, President
- President-elect, (vacant)
- Ms Pauline Wright, Treasurer
- Mr Tass Liveris, Executive Member
- Dr Jacoba Brasch QC, Executive Member
- Mr Ross Drinnan, Executive Member

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

Acknowledgement

The Law Council acknowledges the assistance of its National Criminal Law Committee in the preparation of this submission, as well as input from the Business Law Section's Privacy Law Committee.

Introduction

1. The Law Council is grateful for the opportunity to contribute to the Parliamentary Joint Committee on Intelligence and Security's (**Committee**) review of the amendments introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**Assistance and Access Act**).

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

3. The principal objective of the amendments introduced by the Assistance and Access Act was centred on the legitimate aim of increasing public safety by providing faster access to encrypted data. However, the primary concern of the Law Council is that the measures introduced by the legislation must always be reasonable, necessary and proportionate to that aim by including appropriate safeguards, controls, clarity and certainty in the legislation.

4. The Law Council notes that the Committee has previously conducted an inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (**Assistance and Access Bill**) and the Advisory Report of the Committee was tabled in Parliament on 5 December 2018.[1] In response to the recommendations contained in that report, a number of amendments were introduced by the Government to the Assistance and Access Bill which were then passed by Parliament on 6 December 2018. One of the amendments made to the Assistance and Access Bill required the referral of the Assistance and Access Act to the Committee for review and inquiry, with the Advisory Report of the Committee due in April 2019.

5. The April 2019 Advisory Report of the Committee stated that the focus of that particular inquiry was on 'clarifying the intent of the recommendations made in its 2018 Report and to advise the Parliament on the extent to which those recommendations were addressed'.[2] The Committee acknowledged the many submissions received and the evidence given during both the 2018 inquiry into the Assistance and Access Bill and the 2019 inquiry into the Assistance and Access Act. The Committee went on to state that, given the timing of the then approaching federal election and of this current statutory review now being undertaken by the Committee, the Committee did not to seek to respond to the matters raised in the submissions and evidence given by stakeholders in its Advisory Report dated 4 April 2019.[3]

6. However, the Law Council welcomes the three recommendations that were made by the Committee in that report, namely that:

   (a) section 187N of the Assistance and Access Act be amended to require the Committee's review of the amendments made by the Assistance and Access Act by June 2020;

[1] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Advisory Report, December 2018).
[2] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Advisory Report, April 2019).
[3] Ibid 4 [1.17].

(b) sufficient resources be made available to the Independent National Security Legislation Monitor (**INSLM**) to enable the review of the amendments made by the Assistance and Access Act; and

(c) the Government continues to ensure that the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman (**Ombudsman**) have sufficient resources to ensure that they can properly execute their additional responsibilities under the Assistance and Access Act.

7. The Law Council also acknowledges that the Government amendments did make some of the necessary improvements to the Assistance and Access Bill. In particular, there has been some improvement to record-keeping, inspection and reporting requirements, and have introduced important accountability and oversight measures.

8. However, the Law Council considers that there are a number of outstanding concerns (which the Government amendments have not addressed or have been addressed insufficiently) that are set out in the submission and supplementary submission of the Law Council previously lodged with the Committee dated 23 January 2019[4] and 20 February 2019.[5] These earlier submissions are included as **Attachment A** and **Attachment B** respectively, for the benefit of the Committee.

9. The Law Council maintains the previous recommendations made in earlier submissions which provide comment on the amendments sought to be introduced by the Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 (Cth) (**the Miscellaneous Amendments Bill**).

Reporting by the Commonwealth Ombudsman

10. In addition, the Law Council notes that the inspecting and reporting role held by the Ombudsman appears to be impeded by the ability for the Minister for Home Affairs to delete information in an Ombudsman's report where that information could reasonably be expected to:

(a) prejudice an investigation or prosecution; or

(b) compromise any interception agency's operational activities or methodologies.[6]

11. The Law Council supports the views of the Ombudsman that this power of redaction is unnecessary and is inconsistent with the Ombudsman's role as an independent and impartial office. The Law Council endorses the recommendation of the Ombudsman in this regard and supports its recommendation to the Committee to remove the redaction power contained at subsection 317ZRB(7) of the *Telecommunications Act 1997* (Cth).[7]

[4] Law Council of Australia, Submission No 4 to Parliamentary Joint Commission on Intelligence and Security, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (23 January 2019).
[5] Law Council of Australia, Submission No 4.1 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (20 February 2019).
[6] *Telecommunications Act 1997* (Cth) s 317ZRB(7).
[7] Commonwealth Ombudsman, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (July 2019) 4.

Interaction with foreign laws

12. As per the Terms of Reference of the current inquiry by the Committee, the remainder of this submission will focus on the interaction of the amendments introduced by the Assistance and Access Act with foreign laws – in particular the United States *Clarifying Lawful Overseas Use of Data Act*[8] (**CLOUD Act**) and the European Union's (**EU**) *General Data Protection Regulation* (**GDPR**).[9]

Interaction with the United States CLOUD Act

13. The CLOUD Act was enacted on 23 March 2018 by the passing of the *Consolidated Appropriations Act of 2018* by the 115th United States Congress.[10]

14. The CLOUD Act amends the United States Code (**US Code**) to improve law enforcement access to data stored across borders by, in effect, removing the previous prohibition on providers of electronic communication services from disclosing the contents of electronic communications to foreign governments[11] in certain conditions.[12]

15. The CLOUD Act creates provisions for the provider of an electronic communication service or remote computing service operating in the United States (**US**) to disclose to a 'qualifying foreign government' that is party to an 'executive agreement' with the US the contents of electronic communication of a national or resident of the foreign government directly to a foreign investigative body, such as the Australian Federal Police (**AFP**) in certain circumstances.[13]

16. This would enable, for instance, Facebook (operating from within the US) to provide the contents of electronic communications of an Australian resident that would assist in the investigation of a terrorism-related (or other serious criminal) offence, to the AFP without the AFP having to seek that information through the current process required by the mutual legal assistance treaty (**MLAT**).[14]

17. The CLOUD Act achieves this by amending the *Electronic Communications Privacy Act*[15] (**ECPA**) which regulates the US service provider's disclosure of information about their users, and previously precluded US providers from disclosing user's metadata or communications content to foreign governments.

18. For an Australian law enforcement agency to access the provisions of the CLOUD Act, there needs to be an 'executive agreement' in place between Australia and the US governing access by Australian law enforcement agencies to the data. A requirement of any 'executive agreement' is that the US Attorney General, with the concurrence of the Secretary of State, must determine that the domestic law of Australia 'affords robust substantive and procedural protections for privacy and civil

---

[8] *Clarifying Lawful Overseas Use of Data Act,* HR 4943, 115th Congress (2017-2018).
[9] *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 ('*GDPR*').
[10] *Consolidated Appropriations Act of 2018*, Pub L No 115-141, § 102, 132 Stat 1213.
[11] See *Microsoft Corp. v United States,* 829 F 3d 197, 210 (2d Cir, 2016).
[12] 18 USC § 2713.
[13] Ibid §§ 2702, 2703.
[14] The executive agreements made in accordance with the CLOUD Act only authorise the foreign government to access data of foreigners located outside of the United States.
[15] *Electronic Communications Privacy Act of 1986*, HR 4952, 99th Congress (1985-1986).

liberties in light of the data collection and activities of the foreign government that will be subject to the agreement' as assessed by a number of factors listed.[16]

19. The Law Council notes and agrees with the submission of the Digital Industry Group Inc (which includes representatives from Amazon, Facebook, Google, Oath, and Twitter) on the Assistance and Access Bill, which noted:

> *If our data access regime doesn't contain sufficient safeguards for user privacy, there is a chance that the US Congress, for example, will not approve a treaty with Australia under the CLOUD Act which will interfere with legitimate law enforcement investigations.*[17]

20. Furthermore, the Law Council notes that an executive agreement cannot 'create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data'.[18]

21. Each individual request must be particularised (targeting a specific person, account, address, personal device or other identifier, based on 'articulable and credible facts') and be subject to 'review or oversight by a court, judge, magistrate or other independent authority'.[19]

22. The Law Council considers that the current law in Australia as it relates to storing and accessing telecommunications data will be insufficient to allow Australia to qualify for entry into an 'executive agreement' with the US. This means that law enforcement agencies in Australia will be restricted to seeking access to data held by a service provider in the US through the existing and time consuming MLAT process.

23. The reason for this is that irrespective of what laws Australia may pass, they are insufficient on their own to compel a service provider in the US to do anything not authorised by US law. The sovereignty of both countries is well established and reinforced in this context by each country ratifying the *Budapest Convention on Cybercrime*.[20]

24. Further, the amendments introduced by the Assistance and Access Act do not meet some of the specific criteria required by the CLOUD Act that permit the US to enter an 'executive agreement' with Australia because the legislation arguably fails to meet the following requirements of the CLOUD Act:

    a) the order issued by the foreign government should be specific and identify the relevant individual, account, address or personal device or another specific identifier;
    b) the agreement cannot create an obligation that cannot be fulfilled under US law. In this context, the requirements under the Assistance and Access Act and the CLOUD Act clearly differ, as the US law does not allow for the mandating of the decryption of data as is now permitted under Australian law; and
    c) the CLOUD Act requires that the order issued by the foreign government 'be subject to review or oversight by a court, judge, magistrate or other independent authority prior to, or in proceedings regarding, enforcement of the order' and this

[16] 18 USC § 2523(b)(1).
[17] Digital Industry Group Inc., Submission No 78 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (19 October 2018) 3.
[18] 18 USC § 2523(b)(3).
[19] 18 USC § 2523(b).
[20] *Convention on Cybercrime*, opened for signature 23 November 2011, ETS No 185 (entered into force 1 July 2004).

condition may not be adequately addressed by the amendments introduced by the Assistance and Access Act.

25. It could be argued that section 317ZH places a restriction on a technical assistance notice (**TAN**) or a technical capability notice (**TCN**) from being used to access data or communications that would not be permitted by the issue of a warrant. This may arguably ensure sections 317L and 317T do, in effect, require a TAN or TCN to relate to a specific identifiable 'person, account, address, or personal device'.

26. However, the second, more problematic issue is the inconsistency of the obligations in relation to encryption imposed by the Assistance and Access Act and the US federal law, contained in the *Communications Assistance for Law Enforcement Act 1994* (US) (**CALEA**).[21] This Act does not preclude a carrier from deploying an encryption service for which it does not retain the capacity to decrypt if and when requested by law enforcement to do so. That is, it does not 'mandate that US providers of encrypted communications, devices, and storage services be able to decrypt communications for law enforcement access'.[22] In these circumstances, as argued by Riana Pfefferkorn, Associate Director of Surveillance and Cybersecurity at the Stanford Centre for Internet and Society in the United States, citing §2523(b)(3) of the US Code: 'Any executive agreement with Australia is flatly barred from "creating any obligation that providers be capable of decrypting data"'.[23]

27. Irrespective of the amendments introduced by the Assistance and Access Act in Australia, the provisions of the CLOUD Act will not allow US service providers to provide technical assistance beyond their existing obligations under CALEA. Therefore, even under the existing MLAT scheme a US service provider could not be compelled to comply with a TCN or a TAN issued under the Assistance and Access Act.

28. A further hurdle to Australia being able to form an 'executive agreement' with the US under the CLOUD Act is that the Assistance and Access Act does not provide sufficient requirements for the independent judicial oversight of the issuance of a TAN or a TCN.

29. The Law Council maintains that with the exception of the procedure to issue a TCN, the other measures introduced by the Act are not subject to any form of consideration by an independent judicial officer, notwithstanding the 'general limits' provided by section 317ZH of the Assistance and Access Act. In the case of TCNs, there is a requirement for the exercise of discretion by the Attorney-General who, while Australia's first Law Officer, is not a demonstrably independent party, and is still a member of the Executive.

30. While there is some limited capacity for the courts to make orders in relation to the disclosure, protection, storage, handling and destruction of information obtained pursuant to a TAN, TCN or a technical assistance request (**TAR**),[24] there is no provision for the judicial review of the actual decision to issue the TAN, TCN or TAR.

---

[21] *Communications Assistance for Law Enforcement Act of 1994*, Pub L No 103-414, 108 Stat 4279, codified at 47 USC § 1001-10.
[22] Riana Pfefferkorn, Stanford Centre for Internet and Society, Submission No 35.2 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (13 November 2018) 7.
[23] Ibid.
[24] *Telecommunications Act 1997* (Cth) s 317ZFA.

Interaction with the laws of the European Union

31. The EU's GDPR commenced on 25 May 2018. The GDPR sets a number of restrictions on the processing and transfer of 'personal data'[25] out of the EU, including in response to court orders issued by countries outside of the EU. The GDPR can apply to organisations operating in Australia, where the organisation in question:

    (a) is processing personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not[26]; or

    (b) is offering of goods or services to data subjects in the EU or monitoring of their behaviour as far as their behaviour takes place within the EU.[27]

32. Where the GDPR applies to Australian entities and those entities carrying on business in Australia, it will do so as a matter of law and those in breach of obligations may be subject to law enforcement. Companies subject to the GDPR must ensure that the software, hardware and data centres they use include appropriate safeguards to protect personal data.

33. Notwithstanding that a TCN or a TAN is unable to force a service provider to comply with a notice if it could potentially lead to a 'systemic vulnerability' or 'systemic weakness' to do so, there remains concern about the potential for this to nonetheless occur where a provider attempts to comply, and compliance with the notice potentially compromises the security of personal information.

34. This is contrary to the provisions of the GDPR which requires service providers and other controllers of data to implement appropriate technical and organisational measures so as to implement the data protection principles and provide protection and security for the 'personal data' within the EU. The aims of the GDPR and the requirements of a TCN or TAN to remove or limit the security measures required to protect privacy may be difficult to reconcile.

35. While there is a defence under the Assistance and Access Act to complying with a TAN or a TCN for a 'designated communications provider other than a carrier or carriage service provider' where it would cause contravention of a foreign law,[28] this exemption appears to only apply to acts done outside of Australia. This means that acts done within Australia are not covered by the exemption and therefore compliance with a TCN and TAN may bring the service provider into conflict with a foreign law such as Article 32 of the GDPR.[29]

36. The Law Council has additional concern about the difficulty of defining 'do an act or thing in a foreign country' given the transnational operation of the technology that a TCN or TAN may target. It is conceivable that a TCN or TAN may require a designated communications provider operating in Australia to provide assistance which, although it only requires an employee to do an act or thing in Australia, the software is partially

[25] 'Personal data' is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person: *GDPR* art 4(1).
[26] Ibid art 3(1).
[27] Ibid art 3(2).
[28] *Telecommunications Act 1997* (Cth) s 317ZB(5).
[29] Article 32(1) of the *GDPR* deals with 'Security of processing' and requires a controller and the processor of personal data to 'implement appropriate technical and organisational measures to ensure a level of security appropriate', including, *inter alia*, 'the pseudonymisation and encryption of personal data': *GDPR* art 32(1).

located in the foreign country and/or executed or modified remotely from Australia. This leaves open an ambiguity as to whether the 'doing of the act' (being the execution or modification of the software) is occurring in Australia or the foreign country, leading to ambiguity as to whether the defence applies.

37. Article 48 of the GDPR allows any judgment of a court or tribunal, 'and any decision of an administrative authority' of a country to be recognised within the EU, but only where there is an 'international agreement' in force between Australia and the EU or the applicable Member State of the EU.

38. Personal data may possibly be released from the EU pursuant to an order issued under the Assistance and Access Act under Article 49 of the GDPR, which provides that in the absence of an authorisation being made in accordance with either Article 45 or 46, there is still discretion where 'the transfer is necessary for important reasons of public interest'.[30] It may be that an argument could be made that a serious threat to Australian security would be 'important reasons of public interest'.[31]

39. The difference in approach to the protection of personal data in the EU and Australia is perhaps emblematic of the broader differences being adopted between Australia and the EU in relation to balancing the fundamental human right to privacy and the need for laws that address the need to provide for effective national security measures. In the EU, there is greater protection being given to the fundamental human right of privacy, as reflected in the enactment of the GDPR. However, in Australia, the laws relating to encryption are increasing the capacity of law enforcement to overcome one of the means by which privacy in electronic communications can be protected.

[30] *GDPR* art 49(1)(d).
[31] Such a reasons may also comply with the *GDPR*. This direction deals with the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences and restricts such access to being in accordance with the laws of the EU, and therefore the GDPR.