1 July 2019

Chairperson
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Sir / Madam,

Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 – AIIA Submission

Thank you for the opportunity to provide feedback to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

The Australian Information Industry Association (AIIA) considers both this and the previous reviews undertaken by the PJCIS to be critical in ensuring that the implications of the Act and proposed amendments are subject to comprehensive consultation and scrutiny. The AIIA makes this submission in addition to our joint submission with the Australian Industry Group (Ai Group), Australian Mobile Telecommunications Association (AMTA), Communications Alliance, Digital Industry Group Inc. (DIGI) and Information Technology Professionals Association (ITPA) on 1 July 2019.

The AIIA gives consent for this submission to be published.

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak member body for the ICT industry. AIIA is a not-for-profit organisation that has, since 1978, pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment and drive Australia's social and economic prosperity.

AIIA does this by providing a strong voice for our members' policy priorities, creating a sense of community through events and education, fostering collaboration between industry and government, and curating compelling content and relevant information.

The AIIA National Board and its State Councils embody the diversity of the Australian digital economy, including large Australian companies, multinationals and small and medium-sized enterprises (SMEs).

AIIA members range from start-ups and the incubators that house them, to small and medium-sized businesses including many 'scale-ups' and large Australian and global organisations. They include organisations such as Apple, Adobe, Cisco, Deloitte, DXC, Gartner, Google, IBM, Infosys, KPMG, Lenovo, Microsoft, Optus, Qlik, Salesforce and Telstra, national companies such as Australian Data Centres, Canberra Data Centre, Data#3, KTM Capital, Information Professionals, Technology One, and SMEs including Silverstone Edge, SME Gateway and Zen Enterprise and start-ups such as OKRDY.

Whilst AIIA members represent around two-thirds of the technology revenues in Australia, more than 90% of our members are SMEs.

AIIA Members' response to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act)

As the peak representative body for the Australian ICT industry, the AIIA is a strong advocate for cybersecurity, data protection and information privacy.

As stated in our previous submissions, the Australian ICT industry already provides substantive assistance to law enforcement and intelligence agencies under the Data Retention Regime, the Telecommunications Sector Security Reform and through the pre-existing interception legislation and assistance obligations enshrined in the *Telecommunications Act*.

The AIIA supports ongoing efforts to combat against the use of technologies, including encryption, by anti-state actors, child sex offenders and organised crime to conceal illicit activities. However, the limited consultation on the initial Bill in 2018 and subsequent amendments to the Act that were introduced by the Telecommunications and Other Legislation Amendments (Miscellaneous Amendments) Act 2019 in February 2019 have done little to assuage industry concerns over the potential impact of this legislation.

The AIIA wishes to emphasise that the concerns it has repeatedly expressed in this context are not isolated; there is broad consensus across the ICT industry on the adverse effects this legislation will have for Australian business and economic interests. Prior to the 2019 Federal Election, a series of amendments to the Act were proposed that would have addressed key concerns raised by the AIIA and its industry colleagues. The AIIA encourages the new Government to revisit these amendments and proactively address outstanding concerns raised by the ICT industry in relation to the administration of the Act.

The AIIA is committed to continuing to work with the government to achieve an appropriate balance between fostering technological innovation and the ongoing development of the Australian ICT industry with that of broader security and law enforcement considerations.

AIIA Recommendations:

In addition to the proposed recommendations made to the PJCIS as part of the joint submission by industry groups on 1 July 2019, the AIIA submits the following recommendations:

Recommendation 1: Urgent analysis of the impact of the Act on the Australian ICT industry and export activities is required, as well as a commitment to ongoing monitoring and reporting on these activities.

Recommendation 2: A decision-maker exercising powers under Schedule 1 of the Act should consider the impact of a notice on:

a) the provider's commercial obligations; and,

b) the provider's foreign law compliance obligations to customers in other jurisdictions.

Recommendation 3: Assess and monitor the impact of any withdrawal of multinationals and national companies from the Australian market on the cybersecurity integrity of Government agencies and Australian businesses.

Recommendation 4: Develop a process to identify and manage potential conflict of law scenarios prior to the issuing of a notice.

Recommendation 5: Make provisions for consideration of commercial (e.g. obligations under contract) and legislative non-compliance costs to be faced by a provider in relation to their overseas customers as a result of complying with a Technical Assistance Notice (TAN) or Technical Capability Notice (TCN).

Recommendation 6: Require the Attorney-General to provide a copy of the record of any oral advice to the "Designated Communication Provider" (DCP) in relation to a TCN within 48 hours of giving that oral advice to the DCP in order to minimise disputes arising in relation to the oral advice given by the Attorney-General to the DCP.

Recommendation 7: Require the Director General of Security or a Chief Officer of an interception agency provide a copy of the record of any oral advice given by them to the DCP within 48 hours of giving that oral advice to minimise disputes arising in relation to the oral advice given by the Director General of Security or a Chief Officer of an interception agency.

Recommendation 8: Delete Sections 317W (7) and 317W (8) and 317W (9).

Recommendation 9: Amend section 317WA to require independent assessors to make a binding recommendation to the Attorney-General, whilst also providing a procedure whereby the Attorney-General would retain the ability to issue a notice contrary to the recommendation of the independent assessors but would be required to justify that decision to the relevant DCP and the Inspector-General of Intelligence and Security.

Recommendation 9: The Government to work with industry in developing guidance material for agencies to ensure that community expectations on the important matters of privacy and cybersecurity are afforded appropriate weighting in any agency-based decision-making processes.

Recommendation 10: The Office of the Australian Information Commissioner (OAIC) be afforded direct oversight to ensure compliance with the Australian Privacy Principles (APPs) and report back to Parliament on any breaches of the APPs.

Detailed Overview of AIIA Recommendations

1. Impact on Australian ICT Innovation and Export Activities

The AIIA maintains that, in its current state, the legislation will have a negative impact on Australian ICT activities, both in terms of its ability to innovate and export its expertise. Australian-based products and services captured by the Act are at risk of being perceived as less secure than those in other jurisdictions. The *Perception Survey: Industry views on the economic implications of the Assistance and Access Bill 2018*, undertaken by the Australian Strategic Policy Institute (ASPI Survey) in December 2018, reinforced this view. The ASPI Survey reported that 65% of respondents who are currently exporters or intended to export products and services in the next 12 months had indicated that the Act would have a negative impact on their international business prospects.

This is inconsistent with the Government's ongoing policy commitment to support ICT export opportunities for Australian companies as stated in the *Trade and the digital economy* Report of the Joint Standing Committee on Trade and Investment Growth tabled in September 2018. This also contradicts the goals of *Australia's International Cyber Engagement Strategy 2017* to promote trade and investment opportunities for Australian digital goods and services, and promote the Australian cyber security industry.

Furthermore, the *2016 Performance Review of the Australian Innovation, Science and Research System* conducted by Innovation and Science Australia indicates that Australian businesses are not highly innovative: only 9.2% of Australian businesses are engaged in new-to-market product innovation, which is below the OECD average of 13.3% and well below the average of the top five performing OECD+ countries (21.3% of all firms). This, coupled with the fact that 57% of all respondents to the ASPI Survey anticipated the Act would have a negative impact on their operations within Australia, suggests that local innovation in the ICT sector will suffer as a consequence.

Additionally, the Act will have a negative flow-on effect on Government targets for developing emerging and future technologies for the Australian Defence Force, with cyberspace already acting as a new frontier for defence activities (Defence Industry Policy Statement 2016).

Recommendation 1: Urgent analysis of the impact of the Act on the Australian ICT industry and export activities is required, as well as a commitment to ongoing monitoring and reporting on these activities.

2. Extraterritorial reach

AIIA members consider the extraterritorial reach of the Act will result in multinational businesses withdrawing from the Australian market This would result in both the Australian private and public sectors losing access to those technologies covered by the definition of "Designated Communication Provider" (DCP) in the Act.

As a consequence, multinational AIIA members have already indicated that they are considering withdrawing from the Australian market due to existing contractual and legislative compliance obligations to customers overseas (i.e. GDPR). Under the terms of this legislation, DCPs are only provided with immunity under common law in Australia; it does not extend to overseas jurisdictions.

Recommendation 2: A decision-maker exercising powers under Schedule 1 of the Act should consider the impact of a notice on:

a) the provider's commercial obligations; and

b) the provider's foreign law compliance obligations to customers in other jurisdictions.

Recommendation 3: Assess and monitor the impact of any withdrawal of multinationals and national companies from the Australian market on the cybersecurity integrity of Government agencies and Australian businesses.

3. Conflict of Laws

Section 317E ("Listed acts or things"), read in conjunction with Section 317L ("Technical assistance notices" – outlining the scope of the TANs) and Section 317T ("Technical capability notices" – outlining the scope of TCNs), could result in the issuance of notices to providers that would compel them to undertake acts that have extra-territorial effects, and / or to engage in conduct that might violate foreign law.

In addition, Section 317ZB requires providers to comply with such notices "to the extent the provider is capable of doing so," apparently without regard to the extra-territorial impact or legality of its conduct. Section 317ZL in turn, appears to authorise the service of TCNs and TANs on foreign corporations, while Section 317ZC, which authorises the imposition of civil penalties for non-compliance with a notice, explicitly extends to "acts, omissions, matters, and things outside Australia" – all of which suggest that entities located and doing business outside of Australia might nonetheless be required to comply with such notices.

While the Act does establish a defence for industry non-compliance due to potential conflicts of law, it lacks a mechanism which Australian authorities can identify such conflicts and recognise or resolve them prior to the issue of a notice.

One option would be to apply the same procedure to TANs and TCNs that the proposed new Section 43A of the Surveillance Devices Act 2004 applies to computer access warrants. Section 43A provides that, where a computer access warrant seeks access to data on a computer in a foreign country, the authorising judicial or other authority "must not permit the warrant to authorise that access unless . . . the access has been agreed to by an appropriate consenting official of the foreign country."

Such a provision would significantly reduce the potential for conflicts of law that could otherwise arise when Australian authorities seek access to data that is stored abroad and is protected under domestic law in that country. This rule should also help promote international comity with Australia's allies and respect for fundamental human and civil rights enshrined in foreign-country law.

The lack of a mechanism for identifying and resolving conflicts of laws is not only an omission; it is also a missed opportunity for Australia to further integrate and coordinate law enforcement activities with other nations. For example, the 2018 U.S. *Clarifying Law Overseas Use of Data Act* ("CLOUD" Act) expects that the parties to any international data-sharing agreements adopted pursuant to the Act will have in place mechanisms to resolve conflicts of law. The European Union's regulations on cross-border access to e-evidence also includes such a mechanism.

Recommendation 4: Develop a process to identify and manage potential conflict of law scenarios prior to the issuing of a notice.

4. Reasonableness and the Cost Recovery Model

The cost recovery model proposed only covers those costs associated with complying with a TAN and TCN. The model does not cover other direct and indirect costs that might be incurred by a DCP due to breaches of contractual obligations to overseas customers and for non-compliance with legislation in other jurisdictions (e.g. GDPR).

Recommendation 5: Make provisions for consideration of commercial (e.g. obligations under contract) and legislative non-compliance costs to be faced by a provider in relation to their overseas customers as a result of complying with a Technical Assistance Notice (TAN) or Technical Capability Notice (TCN).

5. Record of advice to be provided to the DCP

Section 317TAA

When the Attorney-General (A-G) issues a TCN to a DCP, the A-G is also required to give the DCP advice relating to the DCP's obligations (either under 317ZA or 317ZB). The A-G can give that advice either orally or in writing. Where the A-G gives the advice orally they must make a written record of the advice within 48 hours of giving the advice. However, the A-G is not required to provide the DCP with a copy of the record of advice. In effect, the DCP is supposed to remember what the A-G told them.

Recommendation 6: Require the Attorney-General to provide a copy of the record of any oral advice to the DCP in relation to a TCN within 48 hours of giving that oral advice to the DCP in order to minimise disputes arising in relation to the oral advice given by the Attorney-General to the DCP.

Section 317MAA (6)

Section 317MAA which relates to TANs issued by the Director-General of Security or a Chief Officer of an interception agency. The Director-General or the Chief Officer of an interception agency is not required to provide a copy of the record of oral advice to the DCP.

Recommendation 7: Require the Director General of Security or a Chief Officer of an interception agency provide a copy of the record of any oral advice given by them to the DCP within 48 hours of giving that oral advice to minimise disputes arising in relation to the oral advice given by the Director General of Security or a Chief Officer of an interception agency.

Section 317W

A TCN must be directed toward ensuring a DCP can give listed help. 317W requires the A-G to invite a DCP to make a submission to the A-G when a TCN is proposed. 317W (7) and (8) address circumstances in which it is proposed to issue a TCN that has the same, or substantially the same, requirements imposed by another TCN that was previously given to the DCP. In these circumstances, the A-G does not have to give the DCP a written notice setting out the proposal and inviting them to make a submission on the proposal.

The A-G's only obligations is to 'consult' the DCP.

Further, if the DCP now has the capability because they were required by the first TCN, then it is not clear why a further TCN seeking the same requirements be needed at all. It is not clear why a TAN would not be issued instead. Therefore, it is not clear what case scenario would necessitate 317W (7) or (8). They would seem to be superfluous provisions and outside the legislative scheme for TANs and TCNs.

Recommendation 8: Delete Sections 317W (7) and 317W (8) and 317W (9).

6. Independent assessors reports

Judicial authorisation and variation of notices provides an independent avenue where the various criteria for granting or varying notices can be assessed. If the Committee is not inclined to support this measure, the AIIA recommends that the procedure contained in section 317WA, for the carrying out an assessment on whether a capability notice should be given or varied, should be amended in two particulars.

The Act currently only requires that the A-G 'have regard to' the independent assessors report. Not requiring the A-G to follow findings in a report by independent assessors, who are asked to assess the validity of a proposed notice, demonstrates their inherently conflicted position as both a decision maker and an interested party.

The Act should be amended to require that the independent assessors make a recommendation to the A-G. Such a recommendation should be based on the assessment of whether a proposed notice, or variation to a notice, satisfies the criteria specified in the Act. To give weight to the assessors' report, the Act should also be amended to require the A-G to follow the assessors' recommendation. Should the A-G, on receipt of a recommendation not to issue a notice, determine that in all the circumstances a notice should be issued, the A-G should be required to notify both the DCP and Inspector-General of Intelligence and Security in writing of their decision, and provide reasons, within a period of 48 hours.

Such a procedure would be in keeping with the administrative process for the review of notices set out in the UK's *Investigatory Powers Act 2016*. It would provide confidence to industry that the regime for the issuing of notices takes seriously all the criteria that must be assessed to determine if a notice or a proposed variation is valid. This recommendation would not delay the process for consideration of notices but would increase transparency and confidence in a process that could have substantial ramifications for companies.

Recommendation 9: Amend section 317WA to require independent assessors to make a binding recommendation to the Attorney-General, whilst also providing a procedure whereby the Attorney-General would retain the ability to issue a notice contrary to the recommendation of the independent assessors but would be required to justify that decision to the relevant DCP and the Inspector-General of Intelligence and Security.

7. Other Issues

AIIA is concerned there is insufficient information on how the "legitimate expectations of the Australian community relating to privacy and cybersecurity" will be:

a) identified at any given point in time;

b) factored into any decision-making process; and

c) given appropriate weighting relative to other considerations, such as national security and law enforcement.

In Australia's 2017 *International Cyber Engagement Strategy*, the Government's goals include advocating for the protection of human rights and democratic principles online.

Recommendation 10: The Government to work with industry in developing guidance material for agencies to ensure that community expectations on the important matters of privacy and cybersecurity are afforded appropriate weighting in any agency-based decision-making processes.

Recommendation 11: The Office of the Australian Information Commissioner (OAIC) be afforded direct oversight to ensure compliance with the Australian Privacy Principles (APPs) and report back to Parliament on any breaches of the APPs.

Mr Ron Gauci
Chief Executive Officer
Australian Information Industry Association
ceo@aiia.com.au
+61 419 538 722