4 February 2019

Mr. Andrew Hastie MP, Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Chair,

***Telecommunications and other Amendment (Assistance and Access) Act 2018*.**

Thank you for the opportunity to provide feedback to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the *Telecommunications and other Amendment (Assistance and Access) Act 2018*.

The AIIA considers this and the previous review by the PJCIS critical to ensuring proper consultation and consideration of the implications of the Act and proposed amendments.
AIIA makes this submission in addition to our joint submission made with the Australian Industry Group (AiGroup), Australian Mobile Telecommunications Association (AMTA), Communications Alliance, Digital Industry Group Inc. (DIGI) and Information Technology Professionals Association (ITPA) on 23 January 2019.

AIIA gives consent for this submission to be published.

Australian Information Industry Association

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 on its 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.

AIIA's National Board and its State Councils embody the diversity of the Australian digital economy, including large Australian companies, multinationals and small and medium sized businesses,

AIIA's 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, Oracle, 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.

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

AIIA members' concerns about the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (the Act)

AIIA is a strong advocate for cybersecurity, data protection and personal information privacy. The industry already provides law enforcement and intelligence agencies with assistance under the Data Retention Regime, the Telecommunications Sector Security Reform and through the workings of interception legislation and assistance obligations under the *Telecommunications Act 1997*.

AIIA supports the continued efforts against the use of technologies including encryption being used by terrorists, child sex offenders, and organised criminals to conceal their illicit activities.

AIIA is committed to working with government to strike the right balance between fostering Australian ICT technology innovation and exports on the one hand and law enforcement activities on the other.

AIIA Recommendations:

In addition to the recommendations made in the joint submission to PJCIS with other industry groups on 23 January 2019, AIIA members have the following recommendations:

Recommendation 1: Urgent analysis of the impact of the Act on Australia's ICT innovation 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 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 A-G 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 317W (7) and 317W (8) and 317W (9).

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

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

Detailed discussion on recommendations from AIIA

1. Impact of Act on Australia's ICT innovation and export activities

AIIA asserts that the impact of the legislation on Australia's ICT export activities will be negative. Products and services of Australian businesses captured by the Act risk being perceived as less secure than those in other jurisdictions. The December 2018 *Perception Survey on the Industry views on the economic implications of the Assistance and Access Bill 2018,* undertaken by the Australian Strategic Policy Institute (ASPI survey), reinforced this view. The ASPI Survey, reported that 65% of the respondents who are currently exporters or wanting to export in the next 12 months indicated that the Bill would have a negative impact on their company's business outside Australia.

This is inconsistent with the Government's fundamental economic policy objective to drive 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 (September 2018). It 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 Australia's cyber security industry.

Furthermore, the 2016 Performance Review of the Australian Innovation, Science and Research System conducted by Innovation and Science Australia highlights 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 countries in the OECD+ (21.3% of all firms). This coupled with the fact that 57% of all respondents to the ASPI Survey expected a negative impact of the Bill for their operations within Australia suggests that local innovation in the ICT sector will go backwards.

Additionally, the Act will have a negative flow on effect on the Australian Government's target of developing emerging and future technologies for the future 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 Australia's ICT innovation and export activities is required, as well as a commitment to ongoing monitoring and reporting on these activities.

2. Extra-territorial reach

AIIA members consider the extraterritorial reach of the legislation is unprecedented and could result in multinational businesses withdrawing from the Australian market. This would result in Australian businesses and Government losing access to the best of technology that will be covered by the definition of "Designated Communication Provider" (DCP) in the Act.

Multinational AIIA members have indicated that they are considering withdrawing from the Australian market due to existing contractual and legislative compliance obligations (e.g. GDPR) to customers overseas. The Act only provides DCPs with immunity at 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 thing), read in conjunction with Section 317L (on the scope of TANs) and Section 317T (on 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 March 2018 U.S. "*CLOUD Act"* contemplates that parties to any international data-sharing agreements adopted pursuant to the Act will have

in place mechanisms to resolve conflicts of law. The EU's proposed E-Evidence Regulation 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 cost 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 breach 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 TAN or 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 A-G 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 Attorney-General 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 317W (7) and 317W (8) and 317W (9).

6. Other issues

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

a) identified at any given point in time,
b) factored into any decision-making process and
c) given an 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 9: The Government to work with industry to develop guidance material for agencies to ensure that community expectations on the important matters of privacy and cybersecurity are afforded the appropriate weighting in agency decision making processes.

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

Kishwar Rahman
GM Policy and Advocacy
Australian Information and Industry Association

k.rahman@aiia.com.au