
# Submission

# to the

# Parliamentary Joint Committee

# On Intelligence and Security (PJCIS)

# on the

# Telecommunications and Other Legislation

# Amendment (Assistance and Access) Bill 2018

October 2018

**Introduction**

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) Bill 2018*.

The AIIA considers this review to be extremely timely and critical. The draft Bill was made public in mid-August and, following a three-week consultation process, a large number of submissions from concerned citizens and organisation were made to the Department of Home Affairs (Home Affairs). A week after submissions closed and with only very minor and cosmetic amendments the Bill was tabled in Parliament. This had raised members' concerns about whether in fact the submissions were given the due consideration.

The AIIA, along with a diverse group of consumer representatives, human rights organisations, industry, technology and telecommunications companies has joined forces under the banner Alliance for a Safe and Secure Internet with a plea to the Australia Government to slow down, stop ignoring the concerns of technology experts, and listen to its citizens about its legitimate concerns with the Bill.

As expressed in our joint press release, (see Attachment A), we are concerned that the rushed processes coupled with the lack of transparency will mean that fundamental issues about privacy erosion and lack of judicial review will not be addressed.

From a policy perspective, creating tools to weaken encrypted systems for one purpose weakens it for all purposes. The Bill does not only target criminals; it puts every Australian at risk. Australians use encryption to buy things online, manage their finances, and communicate personally and professionally. Hospitals, transportation systems and government agencies use encrypted data. If we do not take the time to get this Bill right, in the end, it could be a user's bank account, personal correspondence, or medical records that are compromised.

AIIA makes this submission in addition to our joint submission with Communications Alliance and the Australian Mobile Telecommunications Association (AMTA). We have also made two previous submissions to Home Affairs, which can be viewed here.

AIIA recommendations are highlighted below.

AIIA gives consent for this submission to be published.

**About the Australian Information Industry Association**

*The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. 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 policy priorities; creating a sense of community through events and education; enabling a dynamic network of collaboration and inspiration; and curating compelling content and relevant information.*

*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. We represent global brands including Apple, Adobe, Cisco, Deloitte, DXC, Gartner, Google, IBM, Infosys, KPMG, Lenovo, Microsoft and Oracle; international companies including Optus and Telstra; national companies including Ajilon, Data#3, Technology One, SMEs including Technovate and Silverstone Edge*

*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.*

*Our national board represents the diversity of the digital economy. More detailed information about the AIIA is available on our web site:* www.aiia.com.au

**KEY AIIA Recommendation**

In addition to the explicit recommendations contained in the body of this submission, the AIIA considers that the one day allocated for public hearing is not sufficient for this Bill. More detailed consultation is needed addressing concerns raised by industry as outlined in this paper and our joint submission with Communications Alliance and the Australian Mobile Telecommunications Association.

**AIIA observations and concerns**

AIIA is a strong advocate for cybersecurity, data protection and the protection of 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.

However, AIIA considers that the best way to achieve the outcomes proposed by the draft legislation is through collaboration between government and industry.

In its current form the proposed Bill is broad, complex and ambiguous in many areas. The consultation undertaken by the Department of Home Affairs has not been sufficient to acquit the concerns raised by the general public, industry and other stakeholders. The draft legislation lacks clarity around what it is trying to achieve and many of the proposed new powers are ill-defined. Further consultation and work is required on the development of practical measures and their implementation.

AIIA members' concerns and recommendations for further consideration are detailed below:

**1. Lack of definitions will give rise to uncertainty in application and compliance with the legislation**

a) The draft legislation suffers from a lack of definitional rigour. For example,

> "Systemic weaknesses or vulnerabilities cannot be implemented or built into products or services". The definition of what is meant by "systemic weaknesses or vulnerabilities" is required. At what point does a measure that is introduced become "systemic"?

b) This language seems to indicate that notices can still require development of new methods of access to "whole services," and to individual devices. Reinforcing this view, the Explanatory Memorandum also provides that "the mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built." This suggest that the Australian Government takes the position that building a new capability to access a "target device," service, or software would per se not breach the safeguard set out above. We do not agree with this view. In our view, virtually any tool or

method that can be developed to apply to one service (or instance of a service), or device, can then be replicated to other services and devices. Such tools or methods, once created, would certainly then form a "systemic weakness" for affected services or types of device. Also they have the potential to make service providers liable for breach of contractual arrangements where they have given assurance to customers, including government customers, that their services do not contain a "systemic weakness".

| Recommendation 1 |
| --- |
| AIIA members would like to put forward the following definition:<br>"systemic vulnerability or weakness" means a vulnerability or weakness that could or would extend beyond the specifically targeted device or service that the targeted individual is using and is implemented in such a way that any other user of the same device or service, or any other device or service of the Designated Communications Provider, could or would be affected. |

c) The Bill provides for a broad range of service providers and eligible activities – It might include telecommunication companies, internet service providers, email providers, social media platforms and a range of other "over-the-top" services. It also covers those who develop, supply or update software, and manufacture, supply, install or maintain data processing devices. Notices can be issued to a Designated Communications Provider's supply chain without their knowledge, or to equipment manufacturers that do not handle or have access to the required data. There is a concern that it is so broad as to effectively mean that the legislation can be applied in any context that an agency wishes. It appears to cover anything on the provider's side as well as anything on the consumer's premises.

| Recommendation 2 |
| --- |
| The definition of Designated Communication Provider, eligible activities' and 'listed acts or things' should be narrowed in consultation with providers. |

**2. Lack of transparency in Decision Making will not help to foster collaboration between industry and government in protecting Australian citizens and businesses against crime**

a) The draft legislation introduces a three-tier system of assistance to agencies. While it is easy to see how the Technical Assistance Requests (TARs) differ from the two notices (e.g. voluntary vs. compulsory assistance), it is harder to understand what sets Technical Assistance Notices (TANs) apart from Technical Capability Notices (TCNs), and whether the existing differences justify the reduced safeguards (e.g. the lack of mandatory consultation and oversight by the Attorney-General) under a TAN as well as the additional complexity introduced by having two types of notices. There is a large number of drafting issues around the distinction between TANs and TCNs, that both TANs and TCNs can request DCPs 'build' a certain 'capacity' and that the additional controls and limitations that apply to TCNs are reasonable and desirable.

b) Given the breadth of the powers available under these mechanisms, we believe the safeguards imposed on their use should be equally robust. While the Bill already includes some limitations, we would suggest the following further additions (in addition to those we have suggested above):

c) Where actions are required, they should be limited to those that are "least intrusive." We appreciate that, per Sections 317P, 317V, 317Q(9), and 317X(4), notices can only be issued or varied where considered reasonable, proportionate, practicable and technically feasible. In addition, the Bill should also include an explicit requirement for actions imposed on providers to meet a "least intrusive" standard. That ensures that any steps taken pursuant to a notice will, by default, be those that have the lightest touch on both user privacy and provider's ability to innovate.

d) We would also recommend the extension of the 28-day consultation with service providers that is required prior to imposition of a notice. A period of 60 days is more appropriate given many modern technology systems are deeply complex, and rely on dozens or even hundreds of interlocking subsystems and functions. In order to fully understand the impact of a notified change to the system, more time is likely to be required.

e) It is proposed that Notices will be issued based on the opinions of individuals at the agencies or in their chain of command. However, we note that Notices are not subject to administrative review and there are only limited options to seek judicial relief for Notices that have been issued. We note that the UK Investigatory Powers Act introduced a secondary authorisation from a judicial officer to obtain a technical capability warrant as a result of consultations.

f) The recent Five Eyes statement highlighted that "lawful access should always be subject to oversight by independent authorities and/or subject to judicial review." We should follow the UK Investigatory Powers Act 2016 ("IPA") model which requires that notices must be approved by not only the Attorney-General, but also an independent judge or other judicial authority, who should review notices for both proportionality and necessity.

g) The proposal should also impose a minimum evidentiary threshold for each notice. Requiring a judicial authority to scrutinise claims by issuing officials that safeguard thresholds have been met for each notice, including a review of the evidence available to support that assertion, before agreeing that the notice can be issued would make the safeguards referenced above (e.g., reasonableness, proportionality) more robust. It would also help to establish a global precedent – ultimately protecting Australians' data from indiscriminate interference via similar laws in other countries.

| Recommendation 3 |
| --- |
| AIIA recommends the adoption of a secondary authorisation from a judicial officer to obtain a technical capability warrant like that adopted in the UK Investigatory Powers Act. |

h) Limited scrutiny at a parliamentary level together with delegated decision making further undermine the transparency of the proposed system and introduce scope for abuse, duplication, inconsistency in application and lack of coordinating between agencies. Designated Communication Providers maybe subject to multiple warrants from multiple agencies if there is no centralised coordination through one agency.

| Recommendation 4 |
| --- |
| AIIA recommends that a system for coordinating agency requirements be developed in collaboration between all relevant agencies and industry. |

i) The revised draft Bill now includes certain criteria that the Attorney-General must have regard to for a determination as to what requirements are "reasonable and practicable". Unfortunately, the revised draft Bill still does not include any guidance as to when compliance is "practicable" and "technically feasible" and this ought to be included in the legislation or, at the very least, be addressed, through a regulatory instrument (which is subject to consultation). Such guidance ought to include very specific matters that are to be considered in the determination process and include examples .

| Recommendation 5 |
| --- |
| AIIA members would like to see the development of guidance with key stakeholders on when compliance is "practical" and "technically" feasible. |

j) Section 317ZK(3) provides that DCPs will be reimbursed the "reasonable costs of complying" (unless otherwise agreed). However, AIIA members are concerned that the concept of reasonable cost is wide and not defined but may be interpreted by agencies to only include capital costs and, if at all, limited amounts for operational expenses including overheads where they are relevant. It will be difficult for the "cost negotiator" to have the necessary experience or knowledge to consider the full scope of terms and protections that a service provider may need to address to comply with a Notice. AIIA members are concerned that without industry involvement, the likelihood of costs being accurately calculated by a cost negotiator is unlikely and may lead to protracted discussions between government agencies and providers leaving providers out of pocket. This may have negative consequences for providers that are small businesses.

| Recommendation 6 |
| --- |
| AIIA recommends close industry involvement to help accurately calculate costs. |

k) Where there is a disagreement between a provider and Government on the terms and conditions for compliance with a Notice, there is an option for an arbitrator to be appointed. The arbitrator will be appointed by Australian Communications Media Authority or the Attorney General, with the latter also having the power to issue Notices. AIIA members have concerns that the arbitrator will not be independent.

| Recommendation 7 |
| --- |
| AIIA recommends that checks and balances are put in place to ensure the independence of the arbitrator. |

**3. Operational uncertainty and overreach will create uncertainty for industry**

a) It is not clear in the Bill what requirements can or will be imposed beyond providing access to information at points where it is not encrypted. There is an extensive scope of acts and things that can be requested by the relevant agencies.

| Recommendation 8 |
| --- |
| AIIA members recommend that there be some published guidance on what can be requested and this guidance be updated from time to time in consultation with providers. |

b) The full implication under the Draft legislation of the issuing of Technical Assistance and Technical Capability Notices (Notices) is unclear. Issuing of Notices will require providers to find new ways to provide access to information and providers may not be able to comply with the Notice and still provide end to end encryption. What is not clear is whether "reasonable cost" to provider includes cost to the provider business for failure to provide end to end encryption to its customers as a result of complying with a Notice or whether this will fall under exemptions of civil liability.

| Recommendation 9 |
| --- |
| AIIA members recommend clarifying whether "reasonable cost" to provider includes cost to the service provider for failure to provide end to end encryption to its customers as a result of complying with a Notice or whether this will fall under exemptions of civil liability. |

c) Technical Assistance and Technical Capability Notices may lead to technology vulnerabilities. The Bill includes a specific safeguard that a Technical Assistance or Technical Capability Notice cannot require a designated communications provider to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection. However, a service provider can still be required to (i) provide assistance or build capabilities that impact the security of the service provider's system, products or services in a non-systemic way, or (ii) to implement or build a systemic weakness or vulnerability into something other than "a form of electronic protection".

| Recommendation 10 |
| --- |
| AIIA members note that these latter requirements have the potential to compromise the quality of the service they provide to customers including government customers. |

d) The scope of agency notices is limited to core functions. Core functions can cover a wide range of activities across a number of agencies and the draft legislation also in effect extends these "core functions" to any act or thing that is ancillary or incidental to a relevant objective of the agency. Core functions of an agency change from time to time with Machinery of Government changes. It is also assumed (but which is neither explicitly included or excluded in the Bill) that other government agencies can make requests through a designated interception agency thereby greatly expanding the scope of agency notices.

| Recommendation 11 |
| --- |
| AIIA recommends further discussions on the definition of "core functions" of an agency. |

e) It is extremely important that sensitive commercial information compelled from private industry is only used for the purpose stated in the notice under which it was gathered. For example, information compelled under these provisions should not be used:

- For the development of tools to be used by the Australian Government to compromise further computers
- To test tools developed by the Australian Government with the intention of be widely deployed
- To assist a separate investigation not specifically stated in the notice and supporting warrant
- To be provided to a separate agency outside of the original purpose without further authorization and supporting warrant
- To be provided to any other third party without a lawful need to know that is related to the specific purpose for which the notice was issued.

| Recommendation 12 |
| --- |
| The legislation specifically prohibits the use of the data for purposes outside of the purpose originally stated without further authorisation and supporting warrant, and limits the disclosure of the data to parties with a lawfully established strict need to be informed. This should be reviewed annually by the appropriate ombudsman. |

**4. Conflict of laws risk are high and need to be addressed**

a) Section 317E, 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.

a) In light of these provisions, the risk that compliance with a TAN or TCN will have extra-territorial effects, or conflict with foreign law, is high. While the Bill 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.

b) 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." We welcome this provision, as this should 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.

c) The lack of a mechanism for identifying and resolving conflicts of laws is not only an omission, however – 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 13 |
| --- |
| AIIA recommends a process to identify and manage potential conflict of law scenarios prior to the issuing 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. |

**5. Overlap with existing laws/legislation increases the compliance burden on industry**

a) The Bill introduces side effects and ways to by-pass existing interception and data retention legislation. The explanatory document states that the powers in the Bill "cannot be used to impose data retention capability or interception capability obligations". However, the language in section 317ZH does not prevent a Notice from requiring a service provider that is not a carrier or carriage service provider from facilitating or installing a data retention or interception capability.

b) The enforcement of criminal laws in other countries may mean international requests for data will be funnelled through Australia as the "weakest-link" of our Five Eyes allies. This is because Australia has no enforceable human right protections at the federal level. AIIA members are concerned on the flow on effect of this, that is, a high volume of Notices on providers. Complying with the notices may have a negative effect on these providers especially small businesses who are unlikely to have dedicated resources to deal with such Notices.

c) Australian's trust in a range of digital technologies, service providers, and government may be eroded in an environment where service providers are directed to take actions directed by law enforcement and political officials.

**6. Other issues**

a) It is unclear whether a Regulatory Impact Statement will be published in relation to this Bill.

b) A privacy impact assessment has not been undertaken to understand how the proposed Bill will impact on privacy protection afforded Australian citizens under the Privacy Act 1988

c) There is one area that in our mind has not been sufficiently addressed, that is, how the "legitimate expectations of the Australian community relating to privacy and cybersecurity"

are going to be (i) identified at any given point in time, (ii) factored into any decision making process and (iii) given an appropriate weighting relative to other considerations such as national security and law enforcement.

Kishwar Rahman
GM Policy and Advocacy
Australian Information and Industry Association

K.Rahman@aiia.com.au

ATTACHMENT A

# Slow down, stop and listen – consumers, human rights groups, industry, telcos and technology companies join forces to sound alarm at Government's spyware legislation

3 October 2018

A diverse group of consumer representatives, human rights organisations, industry, technology and telecommunications companies has today joined forces under the banner ***Alliance for a Safe and Secure Internet*** with a plea to the Government to slow down, stop ignoring the concerns of technology experts, and listen to its citizens when they raise legitimate concerns with the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.*

They have united around a call for the so-called "Encryption Bill" to be rejected in its present form.

"This Bill stands to have a huge impact on millions of Australians, so it is crucial that lawmakers reject this proposal in its present form before we sleepwalk into a digital dystopia," said board member of Digital Rights Watch and spokesperson for the Alliance, Lizzie O'Shea.

The Alliance has been formed as the Federal Government has been reluctant to listen to cyber security specialists, technology experts and leaders from civil society organisations. It represents a unique concert of voices – ranging from consumer representatives, human rights groups to industry, telcos and technology companies –who sometimes disagree on policy questions, but have come together for the first time as a unified voice.

"As a group, we are so concerned by the Bill that we feel it is our collective civic duty to use our voices to make sure that the public is aware of the alarming legislation the Federal Government is attempting to rush through Parliament with its Assistance and Access Bill," said O'Shea.

The draft Bill was made public in mid-August and, following a three week consultation process, a large number of submissions from concerned citizens and organisation were received by the Department of Home Affairs. Only a week after the consultation closed the Bill was rushed into Parliament with only very minor amendments, meaning that almost all the expert recommendations for changes to the Bill were ignored by Government.

Communications Alliance CEO, John Stanton, also a spokesperson for the Alliance, said the proposed legislation would put unprecedented powers into the hands of enforcement agencies without judicial or proper Ministerial oversight.

"The scope of this legislation sets a disturbing first-world benchmark and poses real threats to the cyber security and privacy rights of all Australians," he said.

"Instead of trying to ram this legislation through the Committee process and the Parliament, the Government needs to sit down with stakeholders, engage on the details and collectively come up with workable, reasonable proposals that meet the objective of helping enforcement agencies be more effective in the digital age."

The Bill has now been referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), where again processes have been truncated, setting the stage for it to be passed into law within months.

"The rushed processes coupled with the lack of transparency can only mean that expert opinions from Australia and abroad are being disregarded and deep concerns about privacy erosion and lack of judicial review have simply been tossed aside," said O'Shea.

The Bill as it stands would allow Australian law enforcement and security agencies to order technology companies and their staff to facilitate access to an individual's encrypted data and devices without their knowledge or permission and without judicial oversight.

"We should all be worried, because this legislation doesn't only target criminals, it puts every Australian at risk. We use encryption to buy things online, manage our finances, and communicate personally and professionally. Hospitals, transportation systems and government agencies use encrypted data," said O'Shea.

"Creating tools to weaken encrypted systems for one purpose weakens it for all purposes. If the Federal Government succeeds in doing so, it could be your bank account, your personal correspondence, or your medical records that are compromised in the end."

Protecting the public from harm is a priority for all the organisations within the Alliance as well as for the Government. Unfortunately, the reality is that the Bill introduced into the Federal Parliament last week has the potential to make Australians less safe, despite its stated objectives to the contrary.

The Alliance is campaigning for the Government to slow down, stop ignoring the concerns of technology experts, and listen to its citizens when they raise legitimate concerns. For a piece of legislation that could have such far ranging impacts, a proper and transparent dialogue is needed, and care taken to ensure it does not have the unintended consequence of making all Australians less safe.

**Background:**

- Members of the Alliance include ACCAN, Access Now, Ai Group, AiiA, Amnesty International Australia, AMTA, Blueprint for Free Speech, Communications Alliance*****, DIGI, Digital Rights Watch, Future Wise, Hack for Privacy, Human Rights Law Centre, Internet Australia, IoTAA, Liberty Victoria, who together represent consumers, human rights organisations, business, industry and a wide range of technology companies.
- The spokespeople for the Alliance are Lizzie O'Shea, board member of Digital Rights Watch, and John Stanton, CEO of Communications Alliance

*** Important:** *nbn™ is a member of Communications Alliance but has not participated in the preparation of this media release.*

**Media contact:**
Kate Sieper
Impact Group International
kate@impactgroupinternational.com
M: 0466 745 615