Submission to the Department of Home Affairs on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*

September 2018

Joint submission by:
Communications Alliance
Australian Information Industry Association (AIIA)
Australian Mobile Telecommunications Association (AMTA)

7 September 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

ASSOCIATIONS 5

1. INTRODUCTION 6

2. CONCERNS AND SUGGESTIONS FOR FURTHER CONSIDERATION 8

2.1 RELEVANT OBJECTIVES 8

2.2 LISTED ACTS OR THINGS (LATs), SPECIFIED ACTS OR THINGS (SATs) AND LISTED HELP 8

2.3 TECHNICAL ASSISTANCE NOTICE (TAN) VS TECHNICAL CAPABILITY NOTICE (TCN) 9

2.4 DESIGNATED COMMUNICATIONS PROVIDERS (DCPs) AND ELIGIBLE ACTIVITIES 11

2.5 DECISION-MAKING CRITERIA AND PROCESS FOR ISSUING NOTICES 11

2.6 SYSTEMIC WEAKNESSES AND VULNERABILITIES 12

2.7 THREATS TO CYBERSECURITY, PRIVACY AND DATA PROTECTIONS 13

2.8 INTELLECTUAL PROPERTY 14

2.9 INTERCEPTION AND DATA RETENTION 15

2.10 GENERAL LIMITATIONS ON NOTICES AND WARRANTS 15

2.11 INCENTIVES AND OVERSIGHT FOR TECHNICAL ASSISTANCE REQUESTS 15

2.12 OVERALL TRANSPARENCY AND OVERSIGHT 16

2.13 IMMUNITY AND INTERACTION WITH FOREIGN JURISDICTIONS 17

2.14 INTERCEPTION AGENCIES AND DELEGATION OF POWERS 17

2.15 COMPLIANCE AND ENFORCEMENT 17

2.16 OTHER ISSUES 18

3. CONCLUSION 20

EXECUTIVE SUMMARY

This submission on the exposure draft of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Bill or Encryption Bill) is lodged by Communications Alliance*, the Australian Information Industry Association (AIIA) and the Australian Mobile Telecommunications Association (AMTA).

Industry shares Government's desire to protect national security, fight terrorism and crime, enforce law and to enable the relevant agencies to effectively do so in a digital age. Member companies already provide law enforcement and intelligence agencies with various assistance under the Data Retention Regime, the Telecommunications Sector Security Reform (TSSR) and/or through the workings of interception legislation and assistance obligations under the *Telecommunications Act 1997*.

Encryption underpins almost any online activity. Therefore, it is vital to ensure that encryption, and the resultant trust that communications and transactions (in their widest form) are secure and private, are not weakened. Regrettably, encryption is, at times, also being used to conceal illicit and criminal activities and has the potential to significantly hinder the work of intelligence and law enforcement agencies.

The Associations and their members are strong advocates for cybersecurity, data protection and the protection of privacy. Unfortunately, the exposure draft of the Bill bears the very real risk of severely damaging Australia's (and international) cybersecurity and, therefore, to act contrary to its stated aim of increasing security for Australians. The proposed Bill not only creates a schism between security and safety on the one hand and privacy rights on the other, it also – and potentially even more importantly – creates friction between security/safety for the purpose of law enforcement and crime prevention, and security/safety of electronic products and services and, consequently, for our everyday digital lives.

In many places the draft legislation is ambiguous. It lacks definition and clarity as to what it is trying to achieve. The lack of clarity and detail raises significant concerns around intent, actual implementation and, ultimately, legislative overreach. The extraordinarily broad application to almost any person or organisation that has dealings with electronic products and services, irrespective of their location, and the extremely wide scope of acts and things that can be requested of those actors further increase concerns of legislative overreach.

The attempted extraterritorial reach of the legislation is unprecedented. Not only does it have the potential to generate anti-competitive outcomes and to create disincentives for providers to offer products and services to Australians, it also creates significant risks for Australian providers to breach laws in foreign jurisdictions when they are taking action as a result of the requirements of the Bill.

The notice processes created under the draft Bill are prone to the exercise of bias and lack an independent assessment mechanism. Equally concerning is the lack of strong judicial oversight of a piece of legislation that has the potential to significantly impact on society's overall security and the privacy of individuals.

The proposed legislation seeks to break new ground and to set international precedents. Consequently, there is a pressing need to clearly articulate why it is needed and, once consensus is reached, 'to get it right', also bearing in mind international obligations and peer nations' norms. It is imperative that the legislation does not weaken existing cybersecurity structures, carefully balances security and privacy considerations, minimises unintended consequences, and it should be developed within a more holistic framework around cybersecurity, data retention, network security, interception and privacy.

More needs to be done to achieve this. Further consultation (and work on the development of practical measures and their implementation) with all relevant stakeholders, including the Associations and their members, is required prior to the Bill being introduced into Parliament. Industry would welcome the opportunity to review a second exposure draft of the Bill before it is introduced into Parliament.

Once introduced into Parliament, the legislation must be referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for further scrutiny prior to passage.

*NOTE: This submission does not represent the views of NBN Co.

ASSOCIATIONS

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through Industry self-governance.

For more details about Communications Alliance visit http://www.commsalliance.com.au.

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

For more details about AIIA visit https://www.aiia.com.au.

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile carriage service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry.

For more details about AMTA visit http://www.amta.org.au.

1. Introduction

Communications Alliance[1], the Australian Information Industry Association (AIIA) and the Australian Mobile Telecommunications Association (AMTA) (Associations) welcome the opportunity to provide a submission to the Department of Home Affairs (DoHA) on the exposure draft of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Bill or Encryption Bill).

The Associations and their members share Government's objective to strengthen the ability of intelligence and law enforcement agencies to adapt to the digital era. Industry is keen to assist those agencies to protect our society against harmful activities that may be carried out through the use of telecommunications services and other electronic equipment and infrastructure. The companies represented by the Associations already provide significant levels of assistance to intelligence and law enforcement agencies under the Data Retention Regime (*Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*), the Telecommunications Sector Security Reform (TSSR) (*Telecommunications and Other Legislation Amendment Bill 2017*), as well as through the workings of the *Telecommunications (Interception and Access) Act 1979* and Section 313 of the *Telecommunications Act 1997*.

Encryption is a vital part of modern electronic communications as it allows two or more parties to securely and confidentially engage with each other in many forms of communication and online activities. The ability to encrypt (and subsequently decrypt) communications underpins almost every online activity, from chatting on a mobile phone, accessing Government services to online banking, shopping and web browsing. It is fair to say that most of the common online activities that so many Australians engage with numerous times each day would not exist in their current form, or not at all, if not for the security that encryption affords. Therefore, it is important to ensure that encryption, and the resultant trust that communications (in their widest form) are secure and private, are not weakened as our societies increasingly become digitised and 'all online' and does not hinder or disrupt the normal activities undertaken by a law-abiding society.

Industry recognises that encryption is also being used, at times, to conceal illicit and criminal activities, including the exchange of child exploitation material and the potential planning and execution of terrorist acts, and that it has the potential to significantly hinder the investigation, and sometimes prevention, of such activities by intelligence and law enforcement agencies.

It is, therefore, key, to the extent technically possible, to develop a secure framework that safeguards individual freedoms and privacy of individuals, including the privacy afforded through encrypted communications, while simultaneously allowing law enforcement agencies to pursue their goal of upholding and enforcing law and order where there are reasonable grounds to believe that those are at risk. When developing such a framework it is key to recognise that the integrity of security within the supply chain is critical to the security of all services provided to Government, Industry and the public. Supply chain resilience has been a topic of significant focus in the security sector, and any weakening of security in the supply chain will have adverse systemic effects upon all products and services in the chain.

The digitisation of our societies over the past 20 years and the exponential growth in the use of telecommunications services and electronic equipment and services have necessarily required significant changes to the legal basis that underlies the regulation of those services, networks and infrastructures, including the legislative basis for intelligence gathering, law enforcement and cybersecurity. In many instances, the Associations' member companies are voluntarily providing assistance to Australian law enforcement and intelligence agencies in the absence of any legislative framework that directly applies to them. In the past three years alone, the telecommunications industry has seen (or is about to see) three key legislative changes with the introduction of the Data Retention Regime, the TSSR and now the Encryption Bill. This has resulted in a piecemeal approach to various pieces of legislation and resulted in a complex legal environment that is increasingly difficult and costly to navigate for both large and small to

[1] This submission does not represent the views of NBN Co.

medium private sector organisations. It also opens up the potential for unintended consequences and is fraught with the risk that the original intention of a law, e.g. the interception legislation, may be threatened by the practical application of another piece of legislation, e.g. the proposed Encryption Bill, as will be discussed further below.

Importantly, the Bill bears the real risk that the potential gains to be made from improved intelligence gathering may come at the expense of significantly diminishing existing user trust and cybersecurity structures.

Our industry stands at the cusp of even more dramatic changes than those that have characterised the past 20 years, with 5G, the Internet of Things, artificial intelligence and blockchain becoming reality now or on the near future. Consequently, it appears that it may be time to consider a cybersecurity, privacy and law enforcement framework from a more holistic perspective to minimise the number of future 'add-on' pieces of legislation that add further to the already existing cost of compliance, complexity and risks of unintended consequences and circumvention.

2. Concerns and suggestions for further consideration

The proposed legislation is extraordinarily broad in many respects. While some areas of wide scope may be useful and reasonable in the context of the legislation and what it intends to achieve, it is a matter of great concern that the combination of these provisions act to enable intelligence and enforcement agencies to use their powers in ways that cannot be reconciled with the values of modern democracies and the rights to individual freedom and privacy that a democracy ought to afford.

In addition, the draft legislation is very complex and has the potential to introduce unintended consequences and ways to by-pass existing interception and data retention legislation and may assist in by-passing existing legislative checks and balances. Importantly, it bears the risk of undoing much of the progress that has been made over the last decade in strengthening supply chain security and user trust.

2.1 Relevant objectives

The specified acts or things (SATs) that a designated communications provider (DCP) may be requested to do must be "by way of giving help […] in relation to the performance of a function […] so far as the function or power relates to" a list of wide-ranging functions which include the "protection of public revenue". In addition, SATs may also be requested for "a matter that facilitates, or is ancillary or incidental to" any of those wide-ranging functions.[2] It could be argued that almost anything can be deemed ancillary or incidental to the protection of public revenue, thereby creating a very low bar for the application of the powers given to the respective agencies.

To limit this very wide scope at least to some degree, Industry requests that the extension to an act or thing that merely facilitates, is incidental or ancillary to the performance of a function or power of an agency be deleted where it occurs in the draft legislation (e.g. Sections 317G(2)(a)(vi) and (b)(vi), 317L(2)(d) and 317T(2)(a)(ii) and (b)(ii)). Given the potential impact of a SAT, it is not unreasonable to confine the purpose of it to giving help 'in relation to' (note the vagueness of this term) the actual performance of a function or exercise of a power of the requesting agency. Confining the scope in this way would also more adequately reflect the intention of the draft legislation with regard to technical assistance notices (TANs) which are only designed to "request forms of assistance that a provider is already capable of giving, so long as it is of a similar kind to the things specified in 317E".[3]

It is worth noting that the list of functions or relevant objectives in the case of technical assistance requests (TARs) extends to "assisting the enforcement of the criminal laws in force in a foreign country" and "the interests of Australia's foreign relations or the interests of Australia's national economic well-being".[4]

2.2 Listed acts or things (LATs), specified acts or things (SATs) and listed help

Industry is concerned by the extensive scope of acts and things that can be requested by the relevant agencies.

In this context, it is important to understand that the draft legislation differentiates between *specified* acts or things (SATs) and *listed* acts or things (LATs), with LATs only being a subset of SATs, and SATs (not LATs) being the subject of the request or notice that is being issued to a DCP.

While LATs are defined in Section 317E and are already wide in scope, Section 317G(6) (for TARs) and Section 317L(3) (for TANs) broaden this scope even further by stipulating that the list of LATs as per Section 317E is to be viewed non-exclusively. In addition, these sections expand the scope to *any* act or thing as long as that act or thing forms part of the eligible activity of the DCP and relates to, or is ancillary or incidental to, the pursuit of the relevant objectives the

[2] *Telecommunications Act 1997*, new Sections 317L(2) and 317(T)(2) and (3)
[3] p37, Assistance and Access Bill 2018 Explanatory Document
[4] *Telecommunications Act 1997*, new Section 317G(5)(b) and (d)

broad scope of which was discussed above. This mechanism widens the application of requests from *listed* acts or things to *specified* acts of things, which effectively can be any act or thing that is ancillary or incidental to a relevant objective of the agency.

For TCNs, the draft legislation introduces the additional concept of listed help (Section 317T(4)), with listed help now including additional Ministerial powers to determine an act or thing (by legislative instrument) that can be requested and expressly deleting the "removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider"[5] from the list of LATs.

However, this limitation is contradicted by the provisions of Section317T(7) which include *all* LATs and re-introduces the usual concept of SATs into the acts and things that can be requested through a TCN.

It also appears that the drafting of Section 317T(2)(a), which stipulates that the specified act or thing "be directed towards ensuring that the designated communications provider is capable of giving *listed help*" (emphasis added) contradicts the provisions of 317T(7) which broadens the scope to SATs.

Given these inconsistencies, it is not quite clear if the acts or things that can be requested using a TCN (with the exception of acts or things requested under Ministerial powers) are supposed to be different from those of a TAN. Noting the limitations with respect to systemic weaknesses of Section 317ZG, it would seem that the same express removal of item 317E(1)(a) from the LATs ought to apply to TANs. Please refer to the section below for a discussion on the distinction between TANs and TCLs.

Importantly (and independent of the drafting issues highlighted above), Sections 317T(7) to (11) and Section 317ZH place some limits around the kinds of help that can be requested. The inconsistencies and effectiveness of those will be discussed further below.

2.3 Technical assistance notice (TAN) vs technical capability notice (TCN)

The draft legislation introduces a three-tier system of assistance to agencies. While it is easy to see how TARs differ from the two notices (e.g. voluntary vs. compulsory assistance), it is harder to understand what sets TANs apart from 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.

Noting our comments above (see Section 2.2 of this submission), it appears that, ultimately, agencies can request the same acts or things under a TAN and a TCN.

Those acts or things must be in connection with any or all of the eligible activities of the DCP and by way of giving help to the same agencies and in relation to the same relevant objectives. Also the decision making criteria for the issue of TANs and TCNs are the same.

It appears that the key differences are:

- a TCN can only be issued by the Attorney-General in accordance with a request made by the Director-General of Security or the chief officer of an interception agency while a TAN can be issued directly by the latter two;
- a TCP includes a Ministerial power to determine, by legislative instrument, an act or thing that can be requested;
- a TCN must be given in writing whereas a TAN may also be given orally;
- a TCN has a default duration of 180 days rather than 90 days;
- a TCN requires a minimum consultation period of 28 days with the recipient of the notice whereas no consultation is required for a TAN; and
- a TCN has express limits around when it is not effective, i.e. it expressly excludes requests that have the effect of creating or using interception and data retention capabilities or

[5] *Telecommunications Act 1997*, new Section 317E(1)(a)

data, noting that those issues are covered in the *Telecommunications (Interception and Access) Act 1979*. Those limits are absent in the provisions for TANs.

The Explanatory Memorandum (EM) to the draft legislation sheds some light on the intended differences between TANs and TCNs:

> "By contrast, technical assistance notices may contain the listed acts or things in section 317E, as well as additional forms of assistance of a similar kind. The different application of 317E for technical capability notices and technical assistance notices identifies the distinction between circumstances where a provider is already capable of giving assistance and circumstances where a provider might be required to build a capability so that they become capable of giving assistance. It is important that technical assistance notices can request forms of assistance that a provider is already capable of giving, so long as it is of a similar kind to the things specified in 317E. However, in cases where a provider is required to build a capability that goes beyond its own needs, the matters for which this capability can be built should be limited in the legislation and subject to ongoing Parliamentary scrutiny."[6]

Unfortunately, this statement in the EM is not mirrored by the exposure draft in the following respects:

- The extension from LATs to SATs discussed above extends the scope of assistance beyond assistance "of a similar kind" – all that is required for SATs is that they are in connection with (which is already a rather loose term) an eligible activity and give help to an interception agency in relation to the relevant objectives, which do not constitute a high bar;
- The list of things in Section 317E, which finds its application in TANs, includes items (other than (a)) that can be used to request DCPs build 'capabilities' (a term that is not defined) that they do not already have, e.g. item (f) requires "assisting with the testing, modification, development or maintenance of a technology or capability" and item (h) requires "modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider";
- Given the bullet point above and noting the inclusion of SATs into the scope of TCNs, it is not clear how the removal of Section 317E(1)(a) would lead to the desired effect that only TCNs can require DCPs to *build* a capability to enable them to be capable of giving assistance;
- The last sentence of the statement quoted above appears to suggest that items listed in 317E, i.e. listed acts or things, would ordinarily be used for a DCP's own needs. This is not the case. Consequently, if the question whether or not something is being built, modified, developed etc. for a DCP's own needs is relevant for the degree of scrutiny, then *all* requests under TANs and TCNs ought to be subject to ongoing Parliamentary scrutiny; and
- The proposed Section 317ZS requires the Minister to produce an annual report regarding the number of TANs and TCNs issued in a year. There is no ongoing Parliamentary scrutiny provided in the draft legislation in relation to TCNs relating to cases where "a provider is required to build a capability that goes beyond its own needs".

Given the 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, the Associations recommend the removal of TANs from the legislation so that all mandatory notices go through the TCN process which has the additional safeguards of consultation and oversight by the Attorney-General.

Should the TAN remain within the legislation, Industry requests that the process for issuing such notices also include a 28 day consultation period (with the same independent review described above) and impose the same limitations on requests that would have the effect of introducing systemic weaknesses and vulnerabilities as currently included for TCNs (Section 317ZG).

It is key to the design and effective management of the security of an online service that the security architect has a complete view of the relevant systems and its components. The

[6] p37, Assistance and Access Bill 2018 Explanatory Document

possibility that a device, equipment or service supplier will share information, make an alteration, load software or build a capability that is not known to the primary service provider is unacceptable and represents a significant risk to security of the system as a whole. The legislation should be amended to require that an agency issue a TAN (should it remain in the legislation) or TCN only to the primary service provider.

In addition to and independent of the requested removal of the TAN process, the Associations request that the scope of acts or things that can be requested be limited. As discussed, this can be done through a combination of placing greater limits around the relevant objectives of agencies, removing acts and things that are only incidental and ancillary to a function of an agency and by limiting the cases when agencies can issue notices to incidences where the matter that is being investigated or sought to be prevented by an agency is a serious offence.

2.4 Designated communications providers (DCPs) and eligible activities

The broad scope of designated communications providers (DCPs) and eligible activities gives rise to concerns that the draft legislation can effectively be used in almost any circumstance anywhere in the supply chain.

The list of DCPs contained in Section 317C is very extensive and broad in scope. As the list of eligible activities simply mirrors the respective definition for each DCP category, this list is equally wide ranging and covers, for example, the provision of "an electronic service that has one or more end-users in Australia".[7] Given the inclusion of websites in the definition of electronic service, the eligible activities apply to each and every website that a single Australian user accesses (or indeed has ever accessed?) as well as software that has been developed for the use of an electronic service. The eligible activities even cover any service that is ancillary or incidental to the provision of such an electronic service. Similarly, the scope of eligible activities extends to the supply of components that are used, or indeed are only likely to be used, in the manufacture of a facility or customer equipment.

In the context of telecommunications carriers and carriage service providers it should be noted that the supply of eligible services is not limited to supply to the public (as it is often the case, including with regards to the Data Retention obligations) and that no exemption for supply to an 'inner circle' has been granted.

Consequently, the exposure draft envisages a phenomenally wide jurisdiction, geographically and in terms of the providers and services that it covers. It is envisaged that the legislation applies to both sides of the network boundary and it is hard to see what it actually does *not* apply to, i.e. it appears to cover anything on the telecommunications networks side as well as anything at the consumer's premises. It also seeks jurisdiction over almost any over-the-top service and attempts to find application irrespective of the actual use of a service by a (single) Australian user and irrespective of the location of the DCP.

We raise concerns with regards to the enforcement of the legislation further below.

2.5 Decision-making criteria and process for issuing notices

Industry notes with concern that the exposure draft does not contain any further guidance or criteria that would assist the issuing authority with the determination as to what requirements are "reasonable and practicable" and when compliance is "practicable" and "technically feasible".[8]

While the EM provides some guidance on which matters the issuing authority ought to consider, Industry requests that such guidance be provided within the legislation itself, similar to the guidance that is contained in Section 180F of the *Telecommunications (Interception and Access) Act 1979* where seven matters are listed as matters which the decision-maker must have regard to.

[7] *Telecommunications Act 1997*, new Section 313C(b), item 4
[8] *Telecommunications Act 1997*, new Sections 317P and 317V

We also note that under Section 19(b) of the UK *Investigatory Powers Act 2016* the Secretary of State may issue a targeted warrant if he/she "considers that the conduct authorised by the warrant is proportionate to what is being sought to be achieved by that conduct." Similarly, where the term proportionate is used in draft Bill it ought to also describe what that proportionality relates to.

If it is felt that is it not possible to include such guidance into the draft legislation, detailed guidance must be given 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 of the criteria and include examples. In addition, such guidance ought to contain (in a non-exclusive list):

- a requirement to also consider the assessment of reasonableness, proportionality, technical feasibility and practicality as provided by the respective DCP;
- a clear principle that a SAT be requested at the level in the supply chain that is least onerous for the DCP involved and, importantly, with a view to minimising potential additional cybersecurity risks or intrusion into privacy rights;
- a clear pathway to dealing with requests/notices that are likely to have a detrimental effect on a DCP's network, operations or ability to perform other functions required under law, e.g. interception of communications;
- an immunity mechanism for DCPs that take immediate action to protect their networks and services against any further damage by removing a capability or function without prior notification to or agreement by the agency;
- where a DCP was to carry out the requested act or thing, and if the execution of that act or thing were to cause damage to the DCP's infrastructure and/or loss of revenue directly attributable to the act or thing, then a DCP ought to be compensated for the damage and/or loss;
- a right for the DCP to test or otherwise check any software or equipment provided to it to ensure that these do not contain harmful features or otherwise negatively impact the security of the DCP's equipment, network and operations;
- details on the timeframe for the assessment of technical feasibility as an act or thing may be considered technically feasible but only in a very extended timeframe; and
- guidance on how a DCP's size and ability to comply with the obligations are to be assessed.

While consultation with the affected DCP is required for TCNs, the requirement to merely consider a submission that has been received in the process of the consultation is weak. In order to remove any subjectivity from such a critical process (i.e. the interference with the technical capabilities and operations of DCPs and the potential negative effects for cybersecurity and society at large) it is of *vital importance* that a decision to issue a notice and the notice itself are subjected to an ex ante review by an independent agency that possesses sufficient technical expertise to do so.

Without a clear process and decision-making criteria, the very wide powers of the draft Bill seem at odds with the Budapest Convention on Cybercrime (to which Australia is a party) which requires that powers be subject to adequate conditions and safeguards, have sufficient judicial or other independent supervision, clear grounds justifying application of the power, and limitations of the scope and the duration of such powers which take into account the impact of the powers and procedures on the rights, responsibilities and legitimate interests of third parties.

2.6 Systemic weaknesses and vulnerabilities

Section 317ZG aims at ensuring that DCPs cannot be required to "implement or build [or rectify] a systemic weakness, or systemic vulnerability, into a form of electronic protection" (also called 'backdoors' for encryption mechanisms).

Unfortunately, neither the term systemic weakness/vulnerability, nor the term electronic protection has been defined in the exposure draft. It is unclear at what point a requested weakness would become systemic, i.e. would a weakness be systemic when a certain system is

involved or does the concept of systemic revolve around the number of users (potential or actual?) affected by the weakness and, if so, what would a relevant user number threshold be? It is also not clear how vendors of telecommunications network equipment could be required to do a SAT without introducing a systemic weakness or vulnerability given that their products are at the core of most digital communications. Similarly, it is not clear what a weakness or vulnerability would be in the eyes of the requesting agency.

Equally concerning is the lack of a definition for electronic protection. Having regard to the comments in the EM we believe the intention is for electronic protection to have a wide meaning. As an initial suggestion[9] we propose including a definition that captures the following:

> ''Electronic protection means any device, facility, system, software, process, function or information (in whole or part, alone or in combination) that excludes, controls, limits or restricts the operation or control of and/or access to any device, facility, location, system, software, process, function or information, including relating to or used in association with a method of authentication or encryption or any encryption algorithm or key.''

Given the importance of these terms for the draft legislation, we request that Government develop definitions for these terms in consultation with industry experts.

It is also worth noting that while the draft legislation expressly provides that a DCP cannot be required to build systemic weaknesses into its systems or prevent providers from upgrading or fixing systemic weaknesses in their products, it does not prevent an agency from requesting that a DCP build a tailored or targeted weakness into its system. Tailored or targeted weaknesses could still have a broad negative impact on security if this weakness is identified or exploited.

In addition to this lack of clarity, it is key to note that a number of other rules and definitions of the exposure draft and the broad scope of those combined with technical realities mean that the relevant agencies can require DCPs to do SATs that have the same or potentially even worse effects than backdoors as will be argued below.

2.7 Threats to cybersecurity, privacy and data protections

The draft legislation bears the very real risk of severely damaging domestic and international cybersecurity and, therefore, to act contrary to its stated aims. It is key to understand that the Bill not only creates a schism between security and safety on the one hand and privacy rights on the other, it also – and potentially even more importantly – creates friction between security/safety for the purpose of law enforcement and crime prevention, and security/safety of the supply chain and, consequently, for everyday digital lives and everything that depends on or relates to digital existences.

The powers envisaged by the draft legislation appear to permit agencies to instruct manufacturers of devices to add or remove functionalities. Agencies could oblige a device manufacturer to preload (and then conceal) tracking or screen capture software (spyware) on commercial handsets which could be activated remotely. This would effectively by-pass any practical need to break the encryption on communications apps and the like. It appears that such measures would effectively also amount to an interception of communications.

The effects of such requirements are far-reaching and are likely to significantly threaten the trust that users place in their devices and any software that is running on it. For example, if users lose faith in software updates – often designed to patch weaknesses – and fear that those updates may negatively alter the functionalities of their devices, then they may be less inclined to download such updates, thereby harming overall cybersecurity. Such weaknesses are also highly likely to be found and exploited by actors with criminal intentions.

It does not seem unlikely that agencies will seek DCPs to do an act or thing that affects every user of a specific service. While such a request may not be intended to capture every user, technical requirements or the lack of being able to specifically target individual users or groups of users may mean that the agency's request can only be satisfied if the SAT applied to every

[9] We offer this definition as a starting point for discussion. It does not constitute an industry-wide agreed definition.

user of a service. Given the lacking definition of systemic weakness/vulnerability, Industry is concerned that the law may be used to significantly and unduly intrude into the privacy of very large numbers of individuals.

The SAT that may be requested of a DCP includes the installation and use of software. This is alarming as installing and using software may, albeit unintentionally, actually create a systemic weakness or vulnerability or even cause a device to malfunction which would run contrary to the limitations placed by Section 317ZG on the SATs that can be requested by agencies. This risk is even more pronounced were multiple interception agencies to direct that a variety of software be introduced into the same devices or networks.

The Associations consider that the ability for agencies to request the installation of any software constitutes legislative overreach and is unlikely to conform to the principles of reasonableness and proportionality. Installing such software may also cause a DCP to be in breach with its TSSR, data retention or interception obligation.

Given the significant risk of destabilising the Australian communications infrastructure, the ability to request the installation of software ought to be removed from the legislation. If this ability were to remain within the legislation, DCPs must at least be given the opportunity to thoroughly inspect and test the software prior to installation and to provide an opinion consideration of which ought to form part of the decision-making criteria that must be taken into account prior to giving a TCN (or TAN).

In this context we observe that the Bill does not consider the relationship of SATs and a DCP's obligations of notification under the TSSR Regime: Are DCPs required to submit a TSSR notification if the requested act or thing constitutes a significant change to a DCP's network and if the DCP considered that this act or thing constituted a risk to its network or could facilitate unauthorised access and interference?

2.8 Intellectual property

Section 317E(1)(b) lists the provision of technical information as a LAT. Unfortunately, the term technical information is not defined in the Bill. However, the EM states:

> "Technical information could include information about the design, manufacture, creation or operation of a service, the characteristics of a device, or matters relevant to the sending, transmission, receipt, storage or intelligibility of a communication. Examples include source code, network or service design plans, and the details of third party providers contributing to the delivery of a communications service, the configuration settings of network equipment and encryption schemes."[10]

The inclusion of source code and information that would reveal vulnerabilities in the 'definition' of technical information is very concerning. Source code and information relating to vulnerabilities are important intellectual properties and assets of enterprises, and the external sharing of such information may cause great risks to DCPs. Source code may be exploited to build systemic weakness or vulnerabilities (and such vulnerabilities may not be known to downstream communications providers), thereby placing products and services, and ultimately our society at large, at greater security risk.

Industry submits that obtaining source code and information that may reveal vulnerabilities is not necessary or reasonable for the purpose of law enforcement and does not comply with the principle of proportionality. Consequently, the definition of technical information ought to specifically exclude source code and information that would reveal vulnerabilities.

We are also not aware of any other national legislation (including the UK *Investigatory Powers Act 2016*) that would require DCPs to provide source code to law enforcement or interception agencies.

The broad scope of technical information also risks overseas providers of electronic equipment or services to no longer supply Australian companies with advanced and new technologies and

[10] p26, Assistance and Access Bill 2018 Explanatory Document

features if they have to fear that this information can be readily accessed by a large number of agencies.

2.9 Interception and Data Retention

Industry appreciates that Sections 317T(8) to 11 are intended to ensure that TCNs are not to be used to create new or make use of existing interception and data retention capabilities and, thereby, circumvent the workings of the *Telecommunications (Access and Interception) Act 1979*.

However, it appears that other parts of the draft legislation act to either expressly allow interception and access to metadata or could at least be used to do so.

For example, as discussed above, it appears that the loophole created by Sections 317ZH(4) and (5) and the large number of warrants that can be issued that would still meet the relevant objectives of agencies would allow far easier access to metadata kept under the Data Retention Regime than originally envisaged by that Regime.

Similarly, Section 317T(10) only limits the effectiveness of a TCN to the extent that it requires a DCP "to keep, or cause to be kept" what would be considered metadata under the Data Retention Regime. The section does not limit effectiveness where DCPs are required to *disclose* metadata that has been kept under the Regime and the disclosure of which ought to follow the processes established under that Regime.

Importantly, the proposed amendments to legislation enabling computer access warrants expressly allow "intercepting a communication passing over a telecommunications system, if the interception is for the purpose of doing anything specified in the warrant in accordance with this subsection".[11]

2.10 General limitations on notices and warrants

The associations raise concerns with the workings of Section 317ZH. Roughly speaking, Section 317ZH says that a technical assistance notice and technical capability notice cannot require a DCP to do anything for which ordinarily a warrant or authorisation under certain laws would be required. However, Sections 317ZH(4) and (5) then significantly diminish this limitation by stipulating that DCPs must do a SAT if that SAT would "assist in, or facilitate, giving effect to a warrant or authorisation under law".[12] In this context it should be noted that *any* warrant that relates to the relevant objectives of the agency appears to satisfy the requirement, including, for example, a search warrant for drug offences etc.

Even more importantly, in several State jurisdictions of Australia (e.g. Queensland and South Australia), warrants can be issued by a Justice of the Peace (JP). Becoming a JP only requires a minimal amount of training (around 18 hours in Queensland) and no formal education with regards to a subject matter to which the warrant may relate.

Therefore, the combination of the broad scope of relevant objectives of agencies (which include matters that are only ancillary or incidental to those objectives) and the inclusion of warrants as a sufficient condition to allow notices to DCPs serves to create an unacceptable weakening of the limitations that appear to be intended by Sections 317ZH(1) and (2).

2.11 Incentives and oversight for technical assistance requests

The exposure draft does not envisage compensation for assistance provided under TARs. The lack of such compensation creates a clear disincentive for DCPs to provide such voluntary help and stands in stark opposition to the further development of a cooperative cybersecurity framework within which Government and Industry can engage in a dynamic and purpose-oriented manner. The Associations request the inclusion of compensation on the same

[11] *Australian Security Intelligence Organisation Act 1979*, new Section 25A(4)(ba)
[12] *Telecommunications Act 1997*, new Section 313ZH(4)(e) and (f) and Section 313ZH(5)(c) and (d)

(revised) terms (also refer to our comments in Sections 2.5 and 2.16 of this submission) as for TANs and TCNs. DCPs ought not to be required to enter contractual negotiations for the recovery of costs if they are willing to assist agencies.

Importantly, the draft legislation fails to include the number of TARs that must be included in the annual reports to be published by the Minister. It is important that this number be included to provide a transparent picture of the requests/notices made. In addition to the number of TARs made, the Associations request that a split be provided showing how many TARs have been 'complied with' and how many have been 'escalated' to a TAN or TCP and what the reasons were that a DCP gave for not voluntarily providing the assistance. Including this information will allow scrutiny of (and potentially subsequent inquiry into) the practical application of the legislation.

2.12 Overall transparency and oversight

The Associations note with great concern that the proposed amendments to the *Australian Security Intelligence Organisation Act 1979* and other legislation and the proposed secrecy obligations contained the new Section 317ZF of the *Telecommunications Act 1997* effectively mean that an individual employee at an operational level may be given a TCN and that this individual would commit an offence, punishable with a jail sentence of up to five years, by even disclosing to his/her superiors that he/she had received such a notice.

How could a DCP in those circumstances properly assess if the warrant is lawful? Importantly it also creates the risk of people seeking to impersonate agencies and issuing fake TANs or TCNs to individual employees, resulting in the potential for such recipients to hand over confidential or sensitive information or installing spyware or malware for an unauthorised espionage agency.

The secrecy provisions will create an insider threat to all organisations which they will need to counter, to the extent possible at all, by the organisation's own security program.

The inability to share the fact that a TCN has been received will also mean that, where a provider detects some form of abnormality within its systems (which may be the result of the intervention requested by an agency), resources will be wasted on addressing and fixing the detected issue, thereby potentially rendering the entire exercise pointless.

Industry requests that any TAN or TCN be directed to a designated contact within a DCP and that a degree of sharing of information associated with the notice must be permissible. The Bill ought to clearly permit appropriate internal disclosure of a TCN for the purposes of reviewing the notice, consulting on its terms and implementing its requirements.

It is also important to note that the Director-General of Security, the chief officer of an interception agency (or even a more junior staff member to whom the function is delegated) and the Attorney-General can issue notices without judicial oversight. Industry recommends, at the very minimum, that consideration be given to the establishment of a specific judicial oversight regime and possibly the introduction of an Investigatory Powers Commissioner, similar to the measures included in the UK *Investigatory Powers Act 2016*. This will also help with aligning the legislation better with Australia's obligations under the Budapest Convention on Cybercrime.

The annual reporting obligation in Section 317ZS is lacking in detail. To constitute proper oversight the report must include a high-level description of the information or capability sought, the respective category of DCP subject to the notice, whether or not the notice was complied with, whether or not information under warrant has been obtained in reliance on the notice and if so how many warrants, and the cost information per notice as well as overall costs. It also ought to include the information noted in Section 2.12 of this submission.

We also note that the Commonwealth Ombudsman has been given oversight over the Data Retention Regime. The Associations contend that a stronger judicial oversight mechanism is required for the proposed Encryption Bill.

2.13 Immunity and interaction with foreign jurisdictions

The immunities granted by Section 317ZJ of the exposure draft only apply in an Australian context. Given the envisaged application of the legislation to products and services that may affect jurisdictions outside Australia, these immunities are of limited use.

Similarly, the nature of technology and the organisations providing those technologies mean that compliance with a request or notice bears the risk of putting a DCP in breach of the law of a foreign jurisdiction. This may also include, but is certainly not limited to, the EU *General Data Protection Regulation*, the impact of which on Australian organisations is yet to be fully understood.

Therefore, it is *imperative* that the legislation grants an express exemption from compliance where a breach of a law in a foreign jurisdiction would be very likely.

2.14 Interception agencies and delegation of powers

Prima facie, the list of interception agencies contained in the definitions of the proposed new Part 15 of the *Telecommunications Act 1997* appears broad but still reasonable, although it has to be noted that the Australian Federal Police and the Police Forces of each State and the Northern Territory are given the far-reaching powers afforded under the draft legislation.

It should also be pointed out that, when it comes to the practical application of the legislation, all sorts of agencies will seek to have a request or notice issued through one of the listed agencies. While the relevant objective of the issuing agency must still be taken into account, the wide scope of those objectives also means that requests from other agencies that are funnelled though listed interception agencies are likely to occur. This funnelling of requests has already occurred multiple times in relation to the Data Retention Regime. As a Freedom of Information release in January 2016 showed, more than 60 Federal and State Government Departments and agencies as well as several Councils and even greyhound racing organisations have made a request to access metadata. It appears only a question of time before such requests and, in a similar vein, requests to issue requests or notices under the Encryption Bill will be accepted by one of the interception agencies and 'passed on' to DCPs.

While, in theory, the type and number of interception agencies may be acceptable, the envisaged potential for delegation of powers weakens the controls over the powers of the proposed legislation. The Associations recommend that the power to issue a technical assistance notice and to request a technical capability notice from the Attorney-General ought to remain vested in the highest levels of authority within the respective agencies.

2.15 Compliance and enforcement

It is unclear how the Government plans to enforce the proposed legislation for DCPs with an overseas or trans-national presence. For example, if a large social media platform was issued a fine under the new legislation, it could withdraw operations, thereby reducing the range of services to which Australians have access, or simply refuse to pay. In such a scenario it is also questionable whether the level of fines of AUD 10 million would act as a sufficient deterrent given the global revenues of such companies.

Indeed, it may also be pertinent to pose the question if regulation of DCPs without a presence or activity in Australia would actually be constitutional.

Importantly, the obvious difficulties of enforcing the legislation in relation to overseas products or services have the potential to disadvantage Australian providers compared with their international counterparts. The Associations warn that the Bill could have serious anti-competitive effects.

2.16 Other issues

Reimbursement of costs:

Section 317ZK(3) provides that DCPs will be reimbursed the "reasonable costs of complying" (unless otherwise agreed). However, the Associations 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. The intentional distinction between actual costs and reasonable costs is also concerning as it suggests that a person outside the DCP would be well-enough placed to pass judgment over whether or not the costs that the DCP has actually incurred are reasonable. It seems unlikely that an outsider would be in a position to do so.

The draft Bill does also not provide for the recovery of opportunity costs. Depending on what is being required of the DCP, a significant amount of resources may need to be diverted to compliance with a notice. Those resources will not be available for other purposes and, consequently, may mean that more profitable activities cannot be pursued at the same time or speed. The Bill ought to allow for the recovery of opportunity costs.

We also reiterate our concern that TARs are not automatically entitled to a recovery of costs. While the draft legislation allows for contractual arrangements, we request that the legislation include the entitlement to cost reimbursement for TARs. This will provide greater incentives for DCPs if they do not have to be concerned that, in addition to providing the assistance which requires effort and resources, they have to enter into negotiations over costs.

We also again highlight the need for DCPs to be compensated where the execution of an act or thing has led to damages and/or loss.

Effects on competition:

As discussed above, extraterritorial reach of the Bill has the potential to disadvantage Australian providers compared to their international counterparts.

In addition, the Bill also needs to be considered with respect to its effect on national competition: DCPs may be issued with different TCNs with differing requirements. This may place providers which have received complex notices that are difficult to comply with and far-reaching at a competitive disadvantage over those that have not received any notices or less intrusive requests. This can be contrasted with other assistance requirements such as the requirement to provide an interception capability for carriage services which applies equally to all service providers.

Ministerial powers in relation to TCNs:

Sections 317T(5) and (6) give the Minister the power to determine, by legislative instrument, an act or thing for the purposes of a TCN and set out specific matters that the Minister must have regard to when making a determination. To avoid a biased input into the Minister's decision-making process, the Minister ought to be required to consult with Industry before making the respective instrument.

Protection of information:

Industry notes that the mechanisms for protection of information disclosed under the legislation may not be appropriate. The Associations recommend that the legislation invoke different levels of classification of information that is disclosed and allow the DCP to designate the terms of the disclosure.

Information provided by a service provider should be subject to statutory restrictions and a duty to keep confidential and return if obtained by a third party due to a breach of the unauthorised disclosure of information provisions in the Bill.

Variation and revocation of notices:

While the exposure draft envisages the potential variation and revocation of notices and sets out requirements when those can or must take place, it is lacking mechanisms by which a DCP

could seek a variation or revocation on its own accord. Industry requests that such mechanisms be included for all forms of requests/notices.

Written confirmation of a technical assistance notice:

Section 317M allows a TAN to be given orally provided that a written record of the request is being made (within 48 hours). However, the provisions do not specify a clear timeframe within which a copy of the written record of the notice must be given to the DCP and, instead, only requires the copy be provided "as soon as practicable". Given the far-reaching implications of a TAN, a clear, short timeframe for a written record must be stipulated to ensure that the DCP has the correct understanding of what is required of it. Given the record must be created within 48 hours of the notice being given, the law ought to require the issuing authority to provide the written record to the DCP immediately after it has been created. For avoidance of doubt, it ought to be clarified that the written record includes all aspects and content of the oral notice and is not just a mere record of the fact that a notice has been given.

Generally, it ought to be understood that any oral notice bears the risk of impersonation and that it can be difficult to verify the legitimacy of agency.

3. Conclusion

The Associations look forward to continued engagement with Government and other relevant stakeholders on the mutual objective to protect Australians from crime, to enforce law and to enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment.

As highlighted in our submission, the Associations believe that the current exposure draft of the Encryption Bill requires further consultation and substantial work to ensure that the legislation does not weaken existing cybersecurity structures, balances security and privacy considerations and minimises unintended consequences.

We urge Government to engage further with all relevant stakeholders to develop this (and any potential future legislation) with a view to a more holistic framework around cybersecurity, data retention, network security, interception and privacy.

For any questions relating to this submission please contact Christiane Gillespie-Jones on [redacted] or at [redacted].