Dr James Renwick CSC SC
Independent National Security Legislation Monitor
3-5 National Cct, BARTON ACT 2600
Australia

Date 13 September 2019
Reference INSLM Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)

Internet Australia appreciates the opportunity to engage with the Independent National Security Legislation Monitor (INSLM) regarding the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* , which was passed by Parliament in the final sitting of Parliament on 6 December 2018, with little apparent regard to the concerns expressed by hundreds of submissions to the Parliamentary Joint Committee on Intelligence & Security (PJCIS) from Australians and international experts in recent inquiries.

We have provided written submissions to previous PJCIS enquiries on this matter[1] and appeared in hearings within the PJCIS sessions, however we remain disappointed that the modest amendments passed into law have not reflected the gravity of the many problems that the Australian and world expert communities have described in evidence and submissions on this legislation.

Confidential and trusted communications are essential to the ongoing safety, security and efficient use of global Internet communications networks for business, government and personal interactions. Strong encryption technologies ensure confidentiality, and also ensure trust by authenticating that communications are really with the desired recipient and are not being hijacked and redirected by an imposter. Encryption technologies secure web browsing, online banking, and critical public services like electricity, elections, hospitals and transportation.

We understand the concerns of law-enforcement agencies that widespread encryption will make it harder to collect information to prevent or punish terrorists and criminals.

[1] Internet Australia, 2019 Act Review Submission 29, online at https://internet.org.au/news/212-submission-internet-australia-s-submission-to-pjcis-on-assistance-and-access-bill
Internet Australia, 2018 submission on draft Assistance and Access Bill, online at https://internet.org.au/news/209-submission-internet-australia-s-submission-on-draft-assistance-and-access-bill

We must however always be vigilant to ensure well-intentioned measures to assist law-enforcement investigations do not reduce security or privacy for the vast majority of legitimate and law-abiding uses, or retard the ongoing development of future secure and trusted methods of communication. Measures under the banner of 'national security' that weaken the security of communications and the Internet and put the global economy, the critical services we depend on, and the lives of all citizens at greater risk of harm are counterproductive, and should not proceed without considerably more weight placed on the likely harmful consequences to the very people that the Act aims to protect.

We understand the INSLM has been asked to consider whether the Act achieves an appropriate balance, and whether the Act contains sufficient safeguards for protecting the rights of individuals and remains proportionate and necessary. We consider the Act does not contain appropriate balance and safeguards, and is disproportionately tilted towards the perceived requests for enhanced access to communications by law enforcement and national security bodies-requirements which may have the perverse effect of encouraging individuals, business and government to seek less secure and unsafe methods of communicating, to the national and global detriment.

The Government and the Australian public needs to recognise the clear dangers to the security and privacy of ordinary Australians which this legislation enables. The legislation must be amended to protect all parties in the system, including protecting end-users from harmful changes to their devices and applications that are enabled through its rushed legislative process.

About Internet Australia

Internet Australia is the not-for-profit organisation representing all users of the Internet. Our mission – "Helping Shape Our Internet Future" – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations and enable us to provide education and high-level policy and technical information to Internet user groups, governments and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to the development of international Internet policy, governance, regulation and technical development for the global benefit.

Yours Sincerely

Dr Paul Brooks
Chair – Internet Australia
[redacted]

Submission by Internet Australia

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Introduction

This submission is in two major parts.

The first part contains high-level comments and observations on the overall structure of the legislation, and the environment of modern encrypted communications.

The second part contains detailed comments and observations of specific provisions within the legislation that directly address key points regarding the lack of effective checks and balances of the Act:

Summary of Recommendations provided to the PJCIS Inquiry:

Recommendation #1: *We recommend that* ***serious Australian offence*** *defined in s317B be redefined to reference the definition* ***serious offence*** *in s5D of the Telecommunications (Interception and Access) Act 1979.*

Recommendation #2: *We recommend that 'persons (who) manufactures or supplies components' (Items 8 and 11) be removed from the list of 'designated communications providers' in s317C, and that 'manufacturing' and 'supplying' be removed from all other Items where they appear (such as Item 7)*

Recommendation #3 *That the definitions of 'designated communications provider' relating to* ***facilities*** *(S317C (7),(8),(9)) be removed, as they cannot be restricted to a single person as required by the definitions of 'target technology' and s317ZG(4A)-(4C), and in any case 'facilities' are already covered under the items relating to 'carriage services'.*

Recommendation #4: *That a new subparagraph be added to section 317ZF(3) explicitly allowing disclosure (in the case of a notice served on an employee) to the person's employer, or (in the case of a notice served on a contractor) to the contractor's client.*

Recommendation #5: *That subsection 317ZF(3)(e) be expanded to read 'for the purposes of obtaining professional advice, including legal advice, in relation to this Part.'*

Recommendation #6: *That subsection 317ZF(3) be expanded to provide that the costs of seeking legal or other professional advice be borne by, and recoverable from, the issuer of the notice or request.*

Recommendation #7: *That the definitions of 'systemic weakness' and 'systemic vulnerability' be revised, following dedicated consultation with industry on suitable definitions.*

Recommendation #8: *We recommend that the Department consider creating guidance documents regarding 'systemic' weaknesses and vulnerabilities, especially as compared to ordinary weaknesses and vulnerabilities, and engage with industry to jointly assist in describing guidance and process flowcharts to assist the agencies and industry to distinguish when a systemic issue is likely to be created.*

Recommendation #9: *We recommend that a TAN or a TCN should only be issued after a suitable judicial warrant has been obtained, providing evidence and assurance that the safeguards and limitations have been considered by an independent arbiter.*

Recommendation #10: *We recommend that the most dangerous and contentious portions of this ACT, the compulsive Technical Capability Notice, be set aside and removed from legislation until further extensive consultation, round-table meetings and constructive discussion can be had between agencies and the IT industry affected by these laws, seeking to jointly produce a balanced*

outcome where agencies are able to achieve their goals without harming the Australian tech and IT industry.

1 High-Level Comments

1.1 The importance of strong encryption

Encryption is a technical foundation for trust on the Internet. It promotes freedom of expression, commerce, privacy, user trust, and helps protect data from bad actors. Encryption and related techniques are also used to build increased security for financial transactions and to protect the private communications of end users. Encrypted communication is crucial in establishing whether or not data has been tampered with (data integrity), increasing users' confidence that they are communicating with the intended receivers (authentication), and forming part of the protocols that provide the evidence that messages were sent and received (non-repudiation).

Encryption is all around us. It hides usernames and passwords from prying eyes, protects the information exchanged every time a person uses an ATM or swipes a credit-card, conducts a purchase from a smartphone, makes a call from a mobile phone, or presses a key fob to unlock a car. It is a versatile technology, increasingly pervasive in our daily lives, and critical to the security of much of what we do. It is critical for all global commerce, banking, and securities markets. Automatic software updates for billions of end-user devices depend on strong encryption and authentication to prevent the update process being maliciously hijacked.

For these reasons, the Internet development community is actively working to update all Internet communications systems and underlying infrastructure to include strong encryption and authentication by default.

Use of communications systems to carry sensitive and important information is critically dependent on the users of the system being utterly confident that the system can provably guarantee data integrity, confidentiality, and the confirmed identity of the far-end system as being the desired party to communicate with. That confidence does not come from blind faith in the builders of systems, it comes from open inspection of the underlying systems, software and mathematical algorithms by trusted experts who put their skills and reputation on the line proving without doubt that the systems are secure.

Any measure proposed by well-meaning authorities that hinders the ability of communications systems to ensure security, or even hinders the perception by users that the system remains secure, removes the confidence that users require to entrust the system with their confidential and private data. This legislation, and in particular Schedule 1, destroys that confidence by preventing communications systems and services from proving beyond doubt that they remain secure and free from secret undisclosed functionality.

1.2 Encrypted devices and components are crucial to system security

The early focus of law enforcement concerns were directed at making sense of communications streams intercepted 'in-flight' during transmission, accessed through communications interception regimes. The very nature of end-to-end encryption in providing security lies in the endpoints that

generate and decode the encrypted data – the mobile phones, bank terminals, computers, even garage door openers. Reducing the security of these devices – or even increasing doubts about whether the security has been compromised - reduces the ability of citizens and businesses to rely on the entire system to keep them safe.

This legislation is aimed at devices that may be encrypted, and which may store unencrypted versions of messages and other data from before or after transmission. All the concerns of security experts around the dangers of weakening encrypted transmissions apply equally to concerns around weakening the security of users' devices. Users access their devices by supplying a unique key – a password, a PIN, a thumbprint – to unlock the device for their use. **There is no digital lock that only 'good guys' can open and 'bad guys' cannot. "Lawful access" capabilities created using this legislation and the powers provided under a TCN or a TAN will make it easier for others, including criminals and hostile governments, to gain access to sensitive data stored on the same types of devices.**

2 Threshold, scope and proportionality of powers provided for by the Act

2.1 Definition of Serious Australian Offence

This TOLA Act sets a threshold of crimes serious enough for these intrusive powers to be used, by inserting a new definition for **serious Australian offence** in s317B to the *Telecommunications Act 1997* as meaning "an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more or for life."

This is inconsistent with the threshold already defined in s5D of the *Telecommunications (Interception and Access) Act 1979* (TIAA ACT), which defines **serious offence** comprehensively, including offences such as murder, kidnapping, child exploitation and other offences punishable by life or maximum of 7 years imprisonment.

The powers granted under the Assistance and Access Act are highly intrusive, and have been described as being required to help combat highly serious matters such as terrorism and child exploitation ("terrorists, paedophiles and other criminals communicating in secret")[2]. However the inconsistency between these two definitions has created the perverse outcome that crimes considered not serious enough for the TIAA Act are considered to be serious enough for this TOLA Act. The powers are disproportionate for the types of crimes that attract penalties of less than 7 years imprisonment.

We urge you to consider the serious intrusions permitted by the TOLA Act as being disproportionate for the low threshold of offence in the new definition, and to reset the threshold of serious offence

[2] Mike Burgess, "Director-General ASD statement regarding the TOLA Act 2018", online at https://asd.gov.au/speeches/20181212-tola-act-statement.htm

instead to that of s5D of the TIAA Act, which has already been comprehensively reviewed and determined by Parliament to be appropriate for these types of intrusive powers.

Recommendation #1
We recommend that ***serious Australian offence*** *defined in s317B be redefined to reference the definition* ***serious offence*** *in s5D of the Telecommunications (Interception and Access) Act 1979.*

2.2 Scope of Definition of Designated Communications Providers (Component manufacturers)

The new Sect 317C list of types of persons deemed to be *designated communications providers* includes:

- person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia
- person manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia

with their 'eligible activities' being 'a) the manufacture by the person of any such components; or (b) the supply by the person of any such components'

We submit that it is unnecessary, as well as inappropriate and dangerous, to include component manufacturers and component suppliers into this list.

It is *inappropriate*, as a component manufacturer or supplier will likely have no idea if their component 'is likely to be' included in a telecommunications facility or equipment, and even if it is, how it might be used. Nor will they have any significant control of how it might or might not be used. Inclusion of manufacturers and suppliers of 'components' is an example of blanket over-reach by agencies without a clear idea or justification of how powers might be used, when virtually anything from a bolt or screwdriver in a hardware store (that might be used to manufacture something) to an open-source software library might be claimed to fall under these categories.

It is *dangerous*, as compromising components also risks the danger of causing an unforeseen systemic weakness or vulnerability in a system, as an agency cannot know which future systems such a component might be used in, or how. An agency may require a change to a component that might not be deemed to form a systemic weakness or vulnerability in that component – yet that capability would then be incorporated into a future device or facility. The designer and manufacturer of the device or facility will be unaware of the changed function, and the Agency will likely be unaware of the new device or facility, and the changed function may then create a systemic weakness in every device or facility that components of that type are installed into – including any different device or facility that has not connection with communications.

It is *unnecessary*, as the facility operator and equipment manufacturer are also on the list, so any request or notice for assistance could be served on the operator or whole-of-device manufacturer to achieve the same result.

Including *suppliers* of components (as compared with *manufacturers*) is also questionable – retail storefronts and wholesale warehouses can have little impact or information relevant to this subject, and they would have no expectation of being subject to the legislation or able to determine an appropriate response should they receive a notice. Inclusion of these types of persons only serves to drive up costs for these businesses and individuals, as far as those that recognise they might conceivably be caught up under this definition should then incur significant costs in legal advice and developing processes and procedures for dealing with a request from an authority that may never eventuate and can provide no significant assistance.

Recommendation #2

We recommend that 'persons (who) manufactures or supplies components' (Items 8 and 11) be removed from the list of 'designated communications providers' in s317C, and that 'manufacturing' and 'supplying' be removed from all other Items where they appear (such as Item 7)

2.3 Scope of Definition of Designated Communications Providers (Facilities)

The new Sect 317C list of types of persons deemed to be designated communications providers includes:

- the person manufactures, supplies, installs, maintains or operates a facility

- person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia

'Facility' is elsewhere defined in the *Telecommunications Act* as:

> (a) any part of the infrastructure of a telecommunications network; or
>
> (b) any line, equipment, apparatus, tower, mast, antenna, tunnel, duct, hole, pit, pole or other structure or thing used, or for use, in or in connection with a telecommunications network.

The definitions of *systemic weakness* and *systemic vulnerability* prohibit the creation of a weakness or vulnerability unless it is related to a *target technology* connected to a particular person.

Section 317B includes a definition of 'target technology', which covers carriage services, electronic services, software, computer equipment and data processing equipment. Tellingly, the definition does not list any required characteristics for 'facilities', leaving open the possibility of these laws being used to create systemic vulnerabilities and weaknesses in facilities.

It is difficult to understand how a facility might be 'used, or likely to be used' or 'connected' with a particular person, without also being used or connected to other innocent people. By definition, a 'facility' supports all the communications for all the people that flows through that item of infrastructure. In any case, a 'facility' is directly connected with infrastructure of a carrier's network, and so forms part of the infrastructure of a carriage service, and appears to be already covered by the definitions of 'designated communications provider' that relate to carriage services and carriage service providers.

We submit that the prohibition against creating a systemic weakness or a systemic vulnerability makes it illogical for 'facilities' and other items of network infrastructure to be included as designated communications providers – by definition, any exercise of this TOLA Act or any weakness or vulnerability introduced into a *facility* will affect more than one target person, affecting and infringing the rights of numerous innocent people also being served by the target *facility*.

Recommendation #3

That the definitions of 'designated communications provider' relating to facilities (S317C (7),(8),(9)) be removed, as they cannot be restricted to a single person as required by the definitions of 'target technology', and s317ZG(4A)-(4C), and in any case 'facilities' are already covered under the items relating to 'carriage services'.

3 Authorisation processes and decision-making criteria

3.1 Serving process and Confidentiality provisions require clarification

The technical community to which these laws have been targeted have been concerned that individual persons may be targeted to receive notices, and may be required to disclose information or make changes to software or systems without informing their employer[3].

We note the Department of Home Affairs has since clarified that this is not intended[4], which is a welcome clarification, however the legislation still provides that individual persons may be served notices, and it is not clear in the legislation that a person may disclose the notice to their employer. The 'Myths about the Assistance and Access Act' document[5] references s317L, which describes the process of serving a notice on a body corporate, or the process of serving a notice on a designated communications provider – which may be an individual person.

[3] Mozilla may treat Aussie staff as 'insider threats' to code base, Submission to PJCIS, reported at https://www.itnews.com.au/news/mozilla-may-treat-aussie-staff-as-insider-threats-to-code-base-519793

[4] Myths about the Assistance and Access Act, published at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act

[5] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act

Section 317ZF(3)(a) provides that a person subject to a notice may disclose information 'in connection with the administration or execution of this Part' which the Department describes as permitting a body corporate to disclose to an employee, however it does not allow an employee or contactor to inform his/her employer, as a private individual that is served a notice would necessarily need to perform their own administration and execution of the notice to preserve the required confidentiality of the notice.

Recommendation #4

That a new subparagraph be added to section 317ZF(3) explicitly allowing disclosure (in the case of a notice served on an employee) to the person's employer, or (in the case of a notice served on a contractor) to the contractor's client.

Section 317ZF(3)(e) provides that a person subject to a notice may disclose information 'for the purpose of obtaining legal advice in relation to this Part'.

We submit that the restriction to just legal advice is too narrow - a person subject to a notice may need to obtain other forms of professional advice, such as technical advice, in determining how to respond to a notice – and in particular, in determining whether to exercise their rights to request an assessment for a TCN under section 317WA. The restriction of disclosure to just obtaining legal advice disproportionately restricts a person from investigating and reviewing all aspects of understanding and responding to a Notice.

Recommendation #5

That subsection 317ZF(3)(e) be expanded to read 'for the purposes of obtaining professional advice, including legal advice, in relation to this Part.'

3.2 Costs of obtaining advice should be borne by the Agency requiring the activity

Section 317ZK(3)(b) provides that a designated communications provider must comply with the requirement on the basis that the provider does not bear the reasonable cost of complying with the requirement – the provider is permitted to recoup reasonable costs and expenses for complying with a notice from the agency issuing the notice.

Section 317ZF(3)(e) provides that a person subject to a notice may disclose information 'for the purpose of obtaining legal advice in relation to this Part'. A prudent person receiving a notice related to this complex and contentious legislation is likely to require specialist advice, including how their information may also impact their obligations under other laws, such as the *Privacy Act 1988*.

Such advice will come at a (potentially considerable) cost burden to the person - either a natural individual or a corporate body. The cost burden may be sufficiently high as to prevent the person being able to seek legal or professional advice. Sect. 317ZK(3) only allows a provider to recoup the

costs of complying with a notice, but not the costs of evaluating the validity or applicability of the notice before compliance commences, including checking whether the person is correctly described as a relevant designated communications provider for the notice. Sect 317ZK(3) also only applies to recipients of a notice, and not to recipients of a Technical Assistance Request.

We submit that recipients of a notice or a request are not anticipated to be suspected of any form of wrongdoing, and natural justice requires a person should not be required to incur significant out-of-pocket expenses in obtaining advice on dealing with a notice or request from authorities to assist them, or be prevented from seeking and receiving advice due to the cost burden of doing so.

We submit that Sect 317ZF(3), or some other related section, of the TOLA Act should be amended to provide that the costs of seeking and accessing legal or professional advice in relation to the receipt of a notice or a request must be recoverable by the recipient from the issuer of the request or notice.

Recommendation #6

That subsection 317ZF(3) be expanded to provide that the costs of seeking legal or other professional advice be borne by, and recoverable from, the issuer of the notice or request.

3.3 Systemic Weaknesses and Systemic Vulnerabilities

A communications provider cannot be requested to:

- build or implement a systemic weakness or systemic vulnerability into a form of electronic protection, or
- prevent a designated communications provider from rectifying a systemic weakness or a systemic vulnerability in a form of electronic protection.[6]

The definitions of 'systemic' weakness and vulnerability included in the final version of the Act is wholly unsatisfactory – it makes little sense and it uses terms that are not able to be interpreted in ordinary or technical English language:

> ***systemic vulnerability*** means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person.

These is no commonly accepted method of determining what the term 'whole class of technology' might encompass or exclude. For instance, if 'mobile phones' was deemed to be a 'whole class of technology', would a systemic vulnerability be permitted in just a single model, or all model

[6] The Act s317ZG

handsets from a certain manufacturer, be permissible, just because a person used one of those model handsets? If 'tablet computers' was thought to be a 'whole class of technology' would the subset of 'apple iPads' be permitted to have a vulnerability or weakness inserted? This ambiguity, coupled with the non-technical background of agency and government decision-makers, makes such a definition no more useful than having no definition at all.

The ambiguity, and lack of definitions using terms that are meaningful to the providers to which the laws are intended to apply, opens the unreasonable situation that providers are unable to determine by reference to the legislation what activities they are and are not permitted to perform, and further that the issuer of a request or notice will simply define the terms to be whatever they want them to mean at the time – an 'Alice's Adventures In Wonderland'[7] situation where the supposed safeguard provide no real safeguard at all

Recommendation #7

That the definitions of 'systemic weakness' and 'systemic vulnerability' be revised, following dedicated consultation with industry on suitable definitions.

Recommendation #8

We recommend that the Department consider creating guidance documents regarding 'systemic' weaknesses and vulnerabilities, especially as compared to ordinary weaknesses and vulnerabilities, and engage with industry to jointly assist in describing guidance and process flowcharts to assist the agencies and industry to distinguish when a systemic issue is likely to be created.

3.4 'Safeguards' are subjective, and illusionary, and thus are not effective safeguards

The Department in its explanatory material maintains that the legislation includes limitations and safeguards that protect the public and industry against misuse.

We submit that the many of the suggested limitations and safeguards are not effective, since they rely on subjective judgement of persons and decision-makers who will be conflicted and biased in favour of waving through a prospective request or notice.

[7] ""When I use a word," Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean – neither more nor less." "The question is," said Alice, "whether you *can* make words mean so many different things." Lewis Caroll, Alice's Adventures in Wonderland, Chapter 6.

The Department lists 'limitations and safeguards' in its explanation on its website[8].

Considering them in order:

3.4.1 No Systemic Weaknesses

The Department states "notices under the Act cannot require a provider to implement or build systemic weaknesses into electronic protection."

This limitation relies on the definition of systemic weakness and systemic vulnerability, which are themselves problematic. It also relies on the subjective judgement of the decision-maker – a Government officer issuing the request or notice - who has a vested interest in wanting the request or notice to be issued. Historically, many highly damaging systemic vulnerabilities have been introduced by well-meaning persons into global systems, causing significant insecurity and cost to rectify, because the proponents were not able to foresee the future implications of the change – for example, as highlighted by MIT to an earlier PJCIS inquiry, the FREAK and DROWN computer server vulnerabilities were only possible because of US government security mandates[9].

Even with expert technical backing, it is entirely possible for systemic vulnerabilities and weaknesses to be introduced, as even experts may fail to recognise the full implications of a proposed change to systems many years into the future.

3.4.2 Independent Assessments of any new capability

The Department highlights that industry may refer any requirements to build a new capability for review by a technical expert and a retired senior judge (the *assessors*).

This safeguard is illusionary, as both the *assessors* are appointed by the Attorney-General and not by an independent authority, and so may be conflicted in their giving of advice.

Secondly, the Attorney-General is not bound to accept or follow the advice of the assessors.

Thirdly, the process for assessment and reporting described at s317WA does not address what should occur if the two assessors disagree with each other.

3.4.3 reasonable, proportionate, practical and technically feasible.

The Department highlights that decision-makers must be satisfied that a TAR, TAN or TCN is reasonable, proportionate, practical and technically feasible.

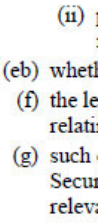
This is not a safeguard, as the decision-makers are the chief officers heads of agencies with a vested interest in having the notice or request issued, and are unlikely to have the deep technology

[8] Assistance and Access: Limitations and safeguards, Department of Home Affairs, online at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-limitations-safeguards

[9] MIT, Submission 32 to PJCIS inquiry into the Assistance AND Access Bill, P4

expertise required to make an assessment of reasonableness or whether an act or thing is technically feasible.

In making sch a subjective assessment, the chief officer must have regard to 9 different factors, such as (s317RA as example):


(ii)

(eb) whetl

(f) the le
relati

(g) such
Secu
relev

We suggest that a chief officer of a law enforcement agency is likely to place entirely different priorities on some of these criteria than an independent judicial officer might, and that this subjective judgement-call by a well-meaning but technically unqualified agency, including '(g) such other matters as ...the chief officer....considers relevant'.

That this supposed safeguard relies entirely on subjective judgement and entirely personal ranking of many conflicting criteria provides little comfort that the requirement forms any type of safeguard.

3.4.4 Additional reporting requirements add to transparency

The Department highlights that the Minister is required to produce a written report each financial year – however it is only to list the numbers of each type of request or notice issued, not any deeper information such as the types of matters they were issued for. In this respect the Ministers' reports will be of lesser value than the reports provided by several agencies to the PJCIS Metadata Retention inquiry occurring concurrently with the PJCIS TOLA Act inquiry, which also detail statistics on the types of investigations that resulted in metadata information requests.

The Department highlights that 'providers may produce transparency reports disclosing the number of notices received in a six-month period.'. Such reports are entirely voluntary on the part of the providers, and so cannot be relied upon to build a picture of the extent of the use of these powers.

Further, the Department notes that providers may also apply for conditional disclosure exemptions to reveal the nature of assistance they have provided. In the explanatory material, this is suggested as a safeguard for technology companies to apply for permission to provide more information to prospective customers in a tender situation.

Industry is unable to rely on this supposed safeguard though, as there is no assurance that such a request would be granted.

The subjective and inherently biased nature of these safeguards can only be mitigated if the judgements and assessment are performed by persons who are independent of the Government, of the Agencies, and of the provider. This assessment can only be performed by a judicial review of the circumstances and the nature of the request or notice, and as such we submit that, at the very least, the compulsive notices (a TAN and a TCN) should require a warrant to be issued.

Recommendation #9
We recommend that a TAN or a TCN should only be issued after a suitable judicial warrant has been obtained, providing evidence and assurance that the safeguards and limitations have been considered by an independent arbiter.

4 Impact on industry and competitiveness

In August 2018 the Australian government banned companies "likely subject to extrajudicial directions from a foreign government that conflict with Australian law"[10] from participating in Australian future telecommunications infrastructure, and in particular from 5G mobile networks. This ban was largely interpreted and confirmed by Huawei and ZTE as primarily aimed at Chinese-controlled equipment providers[11] . This ban follows the Australian government's intervention to

[10] "Government Provides 5G Security Guidance To Australian Carriers", joint media release of Dept. of Communications and the Arts and Department for Home Affairs, 23 August 2018, online at https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

[11] Huawei banned from 5G mobile infrastructure rollout in Australia", ABC News, 23 August 2018, online at http://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438

prevent Huawei Marine building an undersea cable between Australia and the Solomon Islands, also reportedly on national security concerns[12].

This Act has put in place a regime where Australian companies will be subject to the same suspicions, and effectively viewed by the international community as subject to the very same concerns around undisclosed surveillance and surreptitious bypassing of security and privacy functions at the request or direction of the Australian government. Australian manufacturers of communications hardware, developers of Australian communications software systems, every Australian telecommunications provider active in a foreign country, and in fact every Australian website involved in ecommerce to international markets could be suspected to be insecure by international markets. Under the current structure of the Bill, these concerns and suspicions will arise **just by virtue of the legislation existing, even if the legislation is not used.**

Under this Act, Australian authorities may, through a TCN, have required an Australian software or hardware system supplier to modify the system to make it easier for the Australian authority – and any other party who becomes knowledgeable about the capability, including criminal elements and foreign governments through an information leak or by reverse-engineering - to gain access to unencrypted data, and undermine the security of the system. The mere suspicion that this is possible may cause potential purchasers to take their business elsewhere, to purchased systems from other countries where the suppliers are not subject to such requirements.

As the Internet Architecture Board puts it:

This risk might cause some infrastructure providers to relocate, reduce service or even block service to Australian users. Such fragmentation of the Internet is one of the primary concerns we have today as it reduces the value of a global, highly-connected Internet.

...

The ability to compel compromises to the mechanisms that provide security, privacy, and trust on the Internet erodes trust in the Internet as a whole. That erosion, multiplied by the number of political and judicial contexts in which similar approaches might be adopted, represents an existential threat to both the Internet's security and its integrity.[13]

As just one example, the Act provides that operators of a website are designated as subject to the TCN requirements, which may make the site insecure. For example, users of a website can no longer trust that a 'green padlock' that usually designates a secure website is still secure – under a TCN, it is feasible that the website may have been required to falsely display the green padlock without activating the security measures it represents.

---

[12] "Australia takes over Solomon Islands internet cable amid spies' concerns about China", Sydney Morning Herald, 25 Jan 2018, online at https://www.smh.com.au/politics/federal/australia-takes-over-solomon-islands-internet-cable-amid-spies-concerns-about-china-20180125-h0o7yq.html

[13] IAB, Internet Architecture Board (IAB) comments on the Australian Assistance and Access Bill 2018, P3, online at https://www.iab.org/2018/09/10/internet-architecture-board-comments-on-the-australian-assistance-and-access-bill-2018/

Purchasers of goods and services that are supplied through Australian websites are likely to look to suppliers with secure websites in other countries to eliminate the risk that their sensitive details deposited on the website, such as credit card numbers and personal details, are not secure.

The Massachusetts Institute of Technology makes a similar point regarding US-based suppliers:

The marketplace of global technology users, both institutions and individuals, has become sensitized to the risk that national governments may seek to weaken the security of widely-used infrastructure. In the wake of the Snowden disclosures, companies in the United States faced severe scepticism from non-US buyers and increased regulatory pressure from European governments out of a belief that the US national security agencies had compromised the security infrastructure of major US Internet providers.[14]

Statistics from Austrade indicate the value of Australian IT and telecommunications exports in 2016-17 was over AUD$3.2billion[15], and the value of other exports and commerce enabled by Australian websites is incalculable.

In the wake of this Act becoming law, several iconic Australian technology companies including Senetas[16] have expressed that they will need to move out of Australia, and not be subject to this Act, to preserve their business reputation for providing secure systems.

The CEO of Communications Alliance, has said "If no changes are made to either of the new laws, significant damage will be done to the Australian tech sector"..."The erosion of international trust in the Australian tech sector will continue, and that will have impacts on investments and jobs and exports revenue, and the problems contained in the encryption legislation will start to have damaging effects in terms of cybersecurity, and in terms of the rights and privacy of all Australians,"[17].

It will be a national tragedy if Australian exporters of IT systems and software were harmed by international bans and security concerns for precisely the same reasons Australia has chosen to restrict foreign companies from our projects, as a result of this Act just existing.

---

[14] MIT IPRI, Submission on Assistance and Access Bill, P3, online at https://internet.org.au/images/MediaReleases/MIT-IPRI-Comments-AU-Bill-2018-09-10.pdf

[15] "Australia's Export Performance in FY2017", Austrade/DFAT, December 2017, online at https://www.austrade.gov.au/News/Economic-analysis/australias-export-performance-in-fy2017 and http://dfat.gov.au/about-us/publications/trade-investment/australias-trade-in-goods-and-services/Pages/australias-trade-in-goods-and-services-2016-17.aspx

[16] Senetas ready to pull up stumps, March 2019, https://www.innovationaus.com/2019/03/Senetas-ready-to-pull-up-stumps

[17] Encryption fix may now be dead, May 2019, https://www.innovationaus.com/2019/05/Encryption-fix-may-now-be-dead

Recommendation #10

We recommend that the most dangerous and contentious portions of this Act, the compulsive Technical Capability Notice, be set aside and removed from legislation until further extensive consultation, round-table meetings and constructive discussion can be had between agencies and the IT industry affected by these laws, seeking to jointly produce a balanced outcome where agencies are able to achieve their goals without harming the Australian tech and IT industry.

Ends