19 October 2018

Committee Secretariat
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

By email: TOLAbill@aph.gov.au

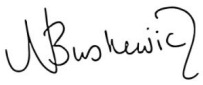
Dear Sir/Madam,

Thank you for the opportunity to provide comments to the Parliamentary Joint Committee on Intelligence and Security on the Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018.

By way of background, the Digital Industry Group Inc (DIGI) includes representatives from Amazon, Facebook, Google, Oath, and Twitter. DIGI members collectively provide digital services to Australians including Internet search engines and other digital communications platforms.

DIGI thanks the Committee for the opportunity to make this submission. If you have any questions or require any additional information, please let me know.

Yours sincerely



Nicole Buskiewicz
Managing Director
DIGI

Introduction

On August 14, 2018, the Government released for Public Exposure a draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the "Bill") together with an Exposure Document, to which DIGI made a submission (attached). A revised Bill was introduced to Parliament ten days following the close of submissions, with only minor amendments that fail to address its potential impacts on public safety, cybersecurity, privacy and human rights, raising concern among industry, consumer and civil society groups.

Protecting the public is a priority for both Government and industry. This is why all of our members have policies that prohibit the use of our services by criminals, terrorists and dangerous organisations. The industry also invests in resources and technology to promptly identify and remove harmful content. And we have worked with Australian law enforcement for many years to provide access to user data when needed and in compliance with applicable laws and international standards to assist with prosecuting criminals.

While DIGI appreciates the challenges facing law enforcement, we continue to have concerns with the Bill, which, contrary to its stated objective, we believe may undermine public safety by making it easier for bad actors to commit crimes against individuals, organisations or communities. We also remain concerned at the lack of independent oversight of Notices and the absence of checks and balances with this legislation, which we discuss in more detail in this submission.

It's important to note that even if the recommendations within this submission were adopted, the Bill proposes extraordinary powers that are unprecedented in scope, and their exercise should be limited to combating serious crimes that pose a grave threat to human life or safety. DIGI does not support the Bill in its current form, and while the recommendations below are intended to make it more workable and protect the safety of Australians online, our overarching recommendation is that Government takes the time to revise its approach in consultation with industry, technical, civil society and security experts.

Implications of the Bill on public safety

The Bill seeks to enable law enforcement and national security agencies to see data and communications in an intelligible form where that data or communication would otherwise be encrypted. The Bill prohibits designated communications providers ('providers') from being required to build or implement a systemic weakness in a form of electronic protection – that is, in their encryption technology. However, as it is the Government's intention that agencies will be able to require providers to help them access data, the Bill anticipates agencies being able to introduce systemic or non-systemic weaknesses into any form of technology.

The problem with this approach is that any act or thing that builds or implements a method for accessing data in a communication or technology system creates a security weakness and a security vulnerability, which can be exploited by a party if they are aware of it and have the means to exploit it. The digital industry spends billions of dollars every year to eliminate data and communication security weaknesses in their products and systems in order to protect the information of their users. Requiring companies to identify or create weaknesses in the processes they use to secure data and communications will make all data and all communications less secure. This would make all users – individuals, corporates, and governments - more vulnerable to exploitation, more susceptible to online attack, and less able to protect themselves online.

This Bill could make average Australians less safe, less secure online and we believe it should be wholly reconsidered. In addition, we have identified the sections of most significant concern in specific comments below.

Specific comments on the Bill

1. **Technical Assistance and Technical Capability Notices (collectively "Notices") that can result in the building and implementation of technology vulnerabilities which facilitate access to data**

Under the Bill, a provider can be required to do many acts or things to facilitate agencies' access to data or communications. Each of these must be directed towards giving help to an agency in relation to the performance of a function or exercise of a power conferred by law upon that agency in so far as the function or power relates to a specified law enforcement or national security outcome. Which agencies can seek Notices and for what purposes is determined by the type of Notice sought.

Even though a TAN or a TCN cannot have the effect of requiring a provider to implement or build a systemic weakness or vulnerability into a form of electronic protection, they can require the provider to:

i. Provide assistance, build or implement capabilities that impact a form of electronic protection in a 'selective' or non-systemic way; or
ii. Remove one or more forms of electronic protection that are used by or on behalf of a provider to protect data; or
iii. Install, maintain, test or use software or equipment given to it by an agency; or
iv. Modify, substitute, or facilitate the substitution of the service provided; or
v. Implement or build a systemic weakness or vulnerability into something other than a form of electronic protection.

It must be remembered that the intention of the Bill is to provide agencies with the means to access otherwise protected information of suspects and gather intelligence or evidence in the

course of an investigation. The powers given to agencies assume that providers have or can develop the means to access protected information in an intelligible form.

The only quarantined act that a provider cannot be required to do is one that has the effect of implementing or building a systemic weakness or vulnerability into the form of electronic protection they use in their product or service. However, as discussed above, any act or thing that builds or implements a method for accessing data in a communication or technology system creates a weakness or vulnerability in that system that can lead to the loss of, or unauthorised access to, information.

A TAN or TCN also risks creating a conflict of law issue for providers that operate multi-nationally. Parliamentarians in other countries will also be watching the progression of this Bill closely. If our data access regime doesn't contain sufficient safeguards for user privacy, there is a chance that the US Congress, for example, will not approve a treaty with Australia under the CLOUD Act which will interfere with legitimate law enforcement investigations.

- **RECOMMENDATION 1**: Notices should not require recipients to build vulnerabilities or weaknesses into their products or services.
- **RECOMMENDATION 2**: Technical Assistance and Technical Capability Notices should only be issued if it is necessary to do so, as determined by an independent judicial authority.
- **RECOMMENDATION 3**: More thought is given to how conflicts of laws will be resolved under the Bill.

2. Judicial Authorisation and Review

Notices will be issued based on the judgment of decision-makers at agencies and the Federal Attorney-General. Notices do not have to be seen or approved by an independent, judicial officer prior to their issuance. Giving decision making responsibility for issuing Notices to executive and political officers puts a high burden upon them to balance the interests of law enforcement and national security, for which they have personal and political responsibility, with the 'legitimate' interests of providers and the legitimate expectations of the Australian community relating to privacy and cybersecurity. What constitutes a legitimate interest of a provider is not defined in the law and will be determined by the official.

Providers will have limited ability to challenge the process of decision making and no ability to challenge a Notice on its merits. In challenging the decision makers' process, providers will not always be aware of facts or criteria that are known to the decision maker in particular because of the highly sensitive information that is relevant to agency capabilities or ongoing investigations which will involve matters of high policy importance, like national security.

- **RECOMMENDATION 4**: The decision to issue the Notice should be made by an independent judicial authority on the basis of evidence and an assessment of clear criteria.

3. Relevant Purposes

Given the extraordinary powers to interfere in information and communication technologies envisaged in the Bill, the scope of the relevant purposes for which Notices can be obtained is broad. Not only do they include the enforcement of Australian criminal matters but also assisting the enforcement of the criminal laws in force in a foreign country. In addition, the powers can be used for the vague and amorphous concept of safeguarding national security however that may be interpreted from time to time.

Most unnecessarily the relevant purposes include the enforcement of laws that impose any pecuniary penalty. This would include any law that provides for a court ordered and collected monetary fine. The breadth of such matters will necessarily cover a range of activity and it is not apparent why the exceptional powers provided by the Notices regime would be required in such circumstances. While it may be argued that the proportionality test would prevent Notices from being issued for 'minor' offences it is not clear how over time law enforcement agencies will prioritise pecuniary penalty infringements.

- **RECOMMENDATION 5**: A more constrained and limited relevant purpose focused on crimes involving risk to human life should be considered and assistance to foreign law enforcement should only involve accessing data held in Australia and should not be a substitute for lawful processes in the foreign jurisdiction.

4. Definitions

The categories of "designated communications provider" to whom Notices can be issued has been defined to be as broad and all-encompassing as possible so as to meet future changes in technologies. It includes any person providing an electronic service with end users in Australia. That would include anyone who operates a website.

It also includes persons providing a service that facilitates, is ancillary or incidental to that electronic service, or persons that develop, supply or update software used, or likely to be used, in connection with that electronic service. This allows Notices to be issued to companies anywhere in the supply chain of a provider, requiring the companies to build and provide compromised or vulnerable software, equipment or services to the service provider without the service provider's knowledge. This is an untenable position for any service provider.

The Bill is lacking in definitions for several critical concepts. There is no definition of 'systemic' as it applies to a 'systemic weakness or vulnerability" nor a prescribed list of "eligible activities" or "listed acts or things". There is no definition of 'legitimate' as it applies to the consideration a decision maker must have to interests of a provider when deciding whether to issue Notices. It is not clear whether commercial interests are legitimate interests or whether the impact of a Notice on other users of a technology would be considered a legitimate interest. Whether a

provider's legitimate interest includes the avoidance of breaching a law of another country by doing an act or thing in Australia is also not clear. What constitutes a 'legitimate interest' is very likely to be a subjective and variable concept capable of situational dispute unless clear guidance is provided in the Bill.

The list of acts and things a provider may be required to do to under a TCN to give help to an agency is effectively unlimited. Section 317T (7) makes clear that the acts or things a provider can be required to do are not limited to the listed acts or things set out in Section 317E. This makes the purpose of a Minister determining acts or things for the purpose of the definition of listed help redundant.

- **RECOMMENDATION 6**: Include a definition for 'systemic' as it applies to a 'systemic weakness or vulnerability' and an exhaustive list of "eligible activities" and "listed acts or things".
- **RECOMMENDATION 7**: Include a definition for 'legitimate' as it applies to the consideration a decision maker must have to interests of a provider when deciding whether to issue Notices.

5. Expansion of Interception and Data Retention Obligations

The Explanatory Memorandum states that the powers in Schedule 1 of the Bill "do not alter a provider's data retention obligations or require a provider to build or retain interception capabilities." However, the language in section 317ZH expressly permits that a TAN and a TCN can require a provider to do an act or thing by way of giving help to an agency in relation to certain matters if the doing of the act or thing would assist in, or facilitate, giving effect to or give effect to a warrant or authorisation under a Commonwealth, State or Territory law. A Notice can therefore require a service provider that is not a carrier or carriage service provider to facilitate or install a data retention or interception capability.

- **RECOMMENDATION 8:** Notices should not be used to impose new data retention and interception capabilities.

6. Exhaustion of all other options by authorised agency

We are concerned by the possibility that an authorised agency might too quickly issue a TAN or a TCN to a designated communications provider before exhausting all other options (within or intra agency).

- **RECOMMENDATION 9**: Authorised agencies should be required to exhaust all other options within their agency and where appropriate consult with other agencies with different levels of expertise before issuing a request to the designated communications provider.