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.

10 September 2018

Department of Home Affairs
4 National Circuit
Barton ACT 2600

By email: AssistanceBill.Consultation@homeaffairs.gov.au

Dear Sir/Madam,

Thank you for the opportunity to provide comments to the Department of Home Affairs on the Telecommunications and Other 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 Department 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. The Bill proposes legislative changes to improve the ability of Australian security, intelligence, customs and law enforcement agencies to access data, transmitted or stored electronically, from local or foreign communications providers.

The proposed changes raise important issues of public safety, cybersecurity, privacy, and human rights. Consequently, we welcome the Government's public release of the Bill for comment and discussion prior to it being tabled in the Parliament.

Relevantly, the digital industry formed the *Reform Government Surveillance*[1] coalition back in 2013 in response to increasing interest within Governments to enact surveillance legislation. The coalition identified and advocates the following important principles when considering legislation to this effect:

1. Limiting Government's Authority to Collect Users' Information

Governments should codify sensible limitations on their ability to compel service providers to disclose user data. These limitations should balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the Internet. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk collection of data or communications.

2. Oversight and Accountability

Governments seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.

3. Transparency About Government Demands

Transparency is essential to an informed evaluation of governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly.

4. Respecting the Free Flow of Information

[1] See: http://www.reformgovernmentsurveillance.com/

The ability of data to flow or be accessed across borders is essential to a robust 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country. Governments should not require service providers to locate infrastructure within a country's borders or operate locally.

5. Avoiding Conflicts Among Governments

In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as bilateral agreements and improved mutual legal assistance treaty (MLAT) processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.

6. Ensuring Security and Privacy Through Strong Encryption

Strong encryption of devices and services protects the sensitive data of our users – including individuals, corporations, and governments. Strong encryption also promotes free expression and the free flow of information around the world. Requiring technology companies to engineer vulnerabilities into their products and services would undermine the security and privacy of our users, as well as the world's information technology infrastructure. Governments should avoid any action that would require companies to create any security vulnerabilities in their products and services.

The intention of this Bill is to facilitate access for law enforcement and security agencies to unencrypted data by securing the cooperation of "designated communications providers" to find ways to access data when it is not encrypted. This may require the provider to identify a weakness in the security of data in their systems or technology and to make that weakness known to those agencies.

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 have concerns with the Bill, which, contrary to its stated objective, may serve to actually undermine public safety by making it easier for bad actors to commit crimes against individuals, organisations or communities. We are concerned at the lack of oversight and the absence of checks and balances with this legislation, which we discuss in more detail in this submission.

Challenges facing law enforcement agencies

As digital technologies have become integrated into everyday life we are increasingly seeing all forms of human behaviour being replicated online and in digital environments. As a result, law enforcement investigations may now involve a digital element and / or interactions that have taken place over an electronic communications platform. This shift has created many challenges for law enforcement, and many in the intelligence community are seeking a broad array of tools and access rights to help them do their job more effectively.

DIGI members have well established and utilised legal processes in place for Australian law enforcement and intelligence agencies to obtain data and request assistance. In the latest 6-month reporting period July-December 2017, members within DIGI responded to over 1,700 government requests for information from Australian law enforcement agencies. Because we recognise that existing international protocols for requesting data from other jurisdictions are outdated and in need of modernisation, we have also been encouraging reform to existing US and other countries' laws - such as the Mutual Legal Assistance Treaty (MLAT) process and bilateral agreements outlined in the US Clarifying Lawful Overseas Use of Data (CLOUD) Act - to provide content when it is available, to non-US law enforcement in a timely way that respects human rights.

It is important to note that the vast majority of requests for information received by DIGI members is for metadata (i.e. non-content), including basic subscriber information and electronic communications records such as Internet Protocol addresses, which would continue to be available even assuming a world with widespread deployment of end-to-end encryption. Content data not encrypted end-to-end on our platforms will also be available.

DIGI members have consistently and actively worked to assist law enforcement with their investigations, including delivering training sessions with law enforcement agencies like the AFP to ensure they have the proper information on how to work effectively with members to ensure requests are processed as expeditiously as possible, in accordance with applicable law and appropriate safeguards. We also regularly engage with senior officials from the Home Affairs Department to discuss emerging crime threats, respective efforts in the counter-terrorism and countering violent extremism space and opportunities for collaboration. Our companies also continue to work with governments around the world on conflicts of law to ensure relevant data, when available, can be provided in a timely, lawful and human rights complaint way.

The importance of strong data protection

Strong data protection, often in the form of data encryption, is an essential foundation for cyber security, and the protection afforded by digital security and strong encryption is an important driver of consumer trust in the Internet. From keeping our banking and health data safe, to

safely storing our private photos and videos, or securely making payments online, encryption makes our digital social and economic lives function.

In his 2015 report on the promotion and protection of the right to freedom of opinion and expression, UN Special Rapporteur on freedom of expression David Kaye concluded "that encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection"[2]. UNESCO's 2016 report on Encryption and Human Rights recognised that "the protection of encryption in relevant law and policy instruments from a human rights perspective is particularly important because encryption makes it possible to protect information and communications on the otherwise insecure communications platform that is the Internet."[3] US Senator Ron Wyden speaking at RightsCon in March 2016 highlighted that "encryption is one of the best defenses an individual has to protect himself or herself in the digital world."[4]

We welcome the Government's acknowledgement that encryption is a "vital part" of the internet, computer and data security, and its importance in supporting Australian economic growth and protecting consumer data. We have concerns, however, that the Bill as currently written could undermine security for all users, including the vast majority of people and businesses who use digital services for good. The proposal for companies to facilitate technical vulnerabilities is of particular concern as it doesn't just create a vulnerability for law enforcement to exploit, it becomes a vulnerability for all, making it easier for criminals to exploit digital technologies to commit crimes.

We have outlined our specific concerns with the Bill below.

Specific comments on the Bill

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

[2] Report on encryption, anonymity, and the human rights framework, https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx
[3] Human Rights and Encryption, http://unesdoc.unesco.org/images/0024/002465/246527E.pdf
[4] Wyden Calls for New Compact for Privacy and Security in the Digital Age, https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-new-compact-for-privacy-and-security-in-the-digital-age

something other than “a form of electronic protection”. These requirements have potential to erode consumer trust and introduce weaknesses that malicious actors could exploit.

2. **Extraterritorial Jurisdiction.** Notices can require service providers to take actions that violate the laws of other countries in which they operate, or which apply to their services because they support customers from other countries. This potentially places service providers in an impossible situation and also potentially jeopardises Australian national security if other governments introduce similar provisions.
3. **No Judicial Authorisation and Review.** Notices can be issued based on the judgment of decision-makers at agencies or the Attorney-General. These Notices may be issued based on facts or criteria that are not known to the recipient, and without full understanding of a technology on the part of an agency.
4. **Notices should be “necessary”, reasonable, proportionate, practicable and feasible.** Notices can be issued to require a service provider, or anyone in the service provider’s supply chain, to assist or develop capabilities to assist law enforcement and national security access data. While the Explanatory Document suggests the issuers of Notices should consider the interests of the service provider and availability of other means to reach that agency’s objectives, this is not the same as a legal requirement that the decision maker be satisfied that issuing the Notice is “necessary”.
5. **Interception capability could be expanded.** The explanatory document states that the powers in the Bill “cannot be used to impose data retention capability or interception capability obligations”. However, the language in the Bill (section 317ZH) does not prevent a Notice from requiring a service provider that is *not* a carrier or carriage service provider from facilitating or installing a data retention or interception capability.

Key recommendations

- Technical Assistance and Technical Capability Notices should only be issued if it is necessary to do so, as determined by an independent judicial authority.
- 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.
- Notices should not require recipients to build vulnerabilities or weaknesses into their products or services.
- Notices should not be used to impose new data retention and interception capabilities.
- Notices should not require recipients to breach laws of other countries that apply to them.

It’s important to note that even if these recommendations were adopted, the Bill proposes extraordinary powers of unprecedented scope, and their exercise should be limited to combating serious crimes that pose a grave threat to human life or safety.

Summary

Given the seriousness of the issues raised by the Bill and potential adverse impact on public safety and the security of online communications generally, DIGI recommends to the Government that it increase dialogue with civil society and industry to find global solutions to the problems identified by the Government to support law enforcement and security agencies in their goal of protecting citizens from harm.

DIGI urges the Government to review the Bill and reflect in it practices that are consistent with established norms of privacy, free expression, and the rule of law as well as conflict of laws, and to specifically adopt the principles advocated by the Reform Government Surveillance Coalition.