Parliamentary Joint Committee on Intelligence and Security
Department of the House of Representatives
PO Box 6021, Parliament House | Canberra ACT 2600
By email: pjcis@aph.gov.au

Monday March 1, 2021

Dear Committee Secretary,

Thank you for the extended opportunity to provide input on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 ("the Bill").

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia, with Google, Facebook, Twitter and Verizon Media as its founding members. DIGI also has an associate membership program and our other members include Redbubble, eBay, Change.org and GoFundMe. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

The Committee should view this Bill as an extension of the *Telecommunications and other Legislation Amendment Act 2018* (Assistance & Access). **That is because the Identify & Disrupt Bill provides law enforcement with greatly expanded powers that increases the incentive to use the tools available to them under the Assistance & Access Act.**

Given this Bill is deeply intertwined with the Assistance & Access Act, DIGI is extremely concerned that there are a number of reviews of that Act that are outstanding at time of writing. The Government has not responded to the Independent National Security Legislation Monitor's (INSLM) review of the Assistance & Access Act. The INSLM found that the Assistance & Access Act is not "proportionate" nor appropriately protective of human rights. In addition, the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the Act has not been completed, despite having a statutory deadline of September 2020. **We do not believe this Bill should proceed until the outstanding concerns under current reviews of the Assistance & Access Act have been addressed.**

From our review of the Bill, we understand that:

- The Bill proposes three new warrants for intelligence agencies: Data Disruption Warrants, Network Activity Warrants and Account Takeover Warrants.
- In the execution of Account Takeover Warrants, the law enforcement officer is authorised to take control of one or more accounts and complete actions including accessing account-based data and adding, copying, deleting, or altering account credentials.
- Access to account-based data is allowed under the warrants if it is necessary to enable evidence to be obtained for the offence / alleged offence. The Bill relates to offenses with penalties of three or more years of jail time.
- The warrants can be executed by law enforcement covertly, without the knowledge of a service provider. As a result, access to the account is obtained through law enforcement "hacking" the service. This is a key difference to the Assistance & Access legislation that includes service provider notifications.
- Although we understand it is not the Government's intent, it is possible that the Bill could be used to impose obligations directly on service providers. For example, both the Data

Disruption Warrants and Network Activity Warrants are tied to “target computers”, which could include a service provider’s systems or servers.
- The Account Takeover Warrant may be used to access an online account regardless of the location of the server, without the knowledge of relevant foreign officials.
- The warrants under this Bill may also be used in conjunction with another warrant under other Australian laws.
- The Bill includes provisions under which law enforcement can compel specified persons to provide reasonable information and assistance to help them carry out a warrant (Surveillance Devices Act ss 64A and 64B(1), Crimes Act s 3ZZVG).

DIGI members routinely cooperate with legitimate law enforcement requests, and work in a number of ways to ensure their users and the broader community have safeguards against harm. **DIGI members have a shared goal with law enforcement to protect safety, however we have concerns that the Bill lacks the robust procedural protections for cyber security, privacy and human rights that Australians and the technology industry would expect.** In our opinion, the Bill does not adhere to the principles of proportionality or necessity.

We therefore outline in this submission a number of broad concerns that the Bill lacks:
- Service provider notifications;
- Cyber security protections;
- Privacy protections;
- Procedural fairness;
- Interoperability with the CLOUD Act & overseas laws;
- Specificity with the scope of services covered;
- Prior judicial authorisation of warrants;
- An appropriate threshold of criminal offenses in line with the Bill’s public positioning.

DIGI looks forward to further engaging with this reform process. Should you have any questions or wish to discuss any of the representations made in this submission further, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

Table of contents

Scope of the Bill

There appears to be a disconnect between the intention of the Government, as evidenced in the Bill's explanatory memorandum, and the drafting of the Bill itself. In particular, there seems to be little to no reference in the explanatory memorandum on the impact of the Bill on service providers. We understand it is the Government's intention that the warrants and assistance orders set out in the Bill do not apply at the service provider level. However, because the drafting in the Bill is extremely broad, it is likely to directly impact service providers, potentially unintentionally, in the following ways:

- **Network Activity Warrants & Data Disruption Warrants:** The explanatory memorandum explains at [16] that: *"network activity warrants will allow the AFP and ACIC to access data in computers used, or likely to be used, by a criminal network…*" It also frequently refers to "devices" in this context and specifically gives examples at the suspect level (e.g. an iPhone 8, serial number 'X' used by suspected criminal 'Y'', or 'all computers used by criminal organisation 'X' at location 'Y'). However, the explanatory memorandum does not explain why the definition of "target computer" (in relation to which a network activity warrant may be issued) in the Bill is so broad, as it is arguably drafted so as to cover a service provider's own systems and servers. It is not clear whether the Government intends for such systems and servers to be caught. If not, it should be clarified in the Bill with limits of necessity and proportionality. A similar issue also exists in relation to Data Disruption Warrants.
- **Assistance orders:** The Bill introduces powers to require specified persons to provide information and assistance that are reasonable and necessary to allow law enforcement to execute the above warrants. The pool of specified persons for the purposes of these assistance orders is extremely broad and could include service providers and their employees. However, there is no reference in the explanatory memorandum to these orders being designed or intended for application to service providers or their employees. Again, if this is not the Government's intention, then it should be clarified in the Bill.
- **Account Takeover Warrants:** In addition, there appears to be a disconnect between the Government's intention about the scope of an Account Takeover Warrant and the drafting in the Bill. The explanatory memorandum explains at [25] that Account Takeover Warrants *"enable[s] the action of taking control of the person's account and locking the person out of the account. Any other activities, such as accessing data on the account....must be performed*

under a separate warrant or authorisation. Those actions are not authorised by an account takeover warrant". However, this is not made explicit in the Bill. In practice, it is difficult to understand how law enforcement could take control of a person's account without accessing the data on that account. If the scope of an account takeover warrant is intended to be confined in this way, then it should be made explicit in the Bill.

- **Relationship with Assistance & Access:** As noted, Bill is inexplicably linked with the Assistance and Access Act. For example, a service provider could be required to provide the same assistance under an Assistance Order under this Bill *and* under a Technical Assistance Notice under the Assistance and Access Act. However, assistance requested under this Bill would not receive the same protections and processes built into the Assistance & Access Act. Again, it is unclear whether this is the Government's intention, given there is no reference to the Assistance & Access Act in the explanatory memorandum. The intended relationship between this Bill and Assistance & Access Act must be clarified, and take into account recommendations from the review of the Act from the INSLM and PJCIS.

The need for greater clarity on the Bill's scope in the above areas is critical; these issues raise serious technical and legal challenges, detailed later in this submission.

Lack of service provider notifications

We understand that the Account Takeover Warrants can be executed by law enforcement covertly, without the knowledge of a service provider. As a result, access to a user's account could be obtained through law enforcement "hacking" or otherwise manipulating the service unilaterally. This is a key difference to the Assistance & Access Act that includes a service provider notification of the access request.

Furthermore, we understand that Account Takeover Warrant is designed to be used in circumstances where law enforcement officers have a person's account credentials, but the person has not given his or her permission for law enforcement to use the account.

It is essential that a service provider be notified before the issuance of an Account Takeover Warrant. A lack of service provider notification compromises the security of users of the service provider's service. Law enforcement "hacking" or otherwise manipulating a service in order to obtain access will threaten the security of other users of that service. In order to complete an account takeover, law enforcement will need to identify and exploit a vulnerability in the digital service; there is nothing to prevent this vulnerability being exploited by bad actors. This will cause other security risks to those users and possible crimes.

Assessing the impact on encryption

In assessing the likely impact of the Bill, it is important to examine whether the powers granted to law enforcement are necessary and proportionate to keep Australians safe. One important consideration in this regard is how the new powers for law enforcement contemplated in this legislation would impact the efficacy of end-to-end encryption.

As mentioned, the Committee should view this Bill as an extension of the Assistance & Access Act. The Identify & Disrupt Bill provides law enforcement with greatly expanded powers that increases their incentive to use the tools available to them under the Assistance & Access Act. There are also clear intersections between the Bill and the Act. Given that, DIGI is extremely concerned that there are a number of reviews of that Act that are outstanding at time of writing. The Government has not responded to the Independent National Security Legislation Monitor's (INSLM) review of the Assistance & Access Act. The INSLM found that the Assistance & Access Act is not "proportionate" nor appropriately protective of human rights. In addition, the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the Act has not been completed, despite having a statutory deadline of September 2020. We do not believe this Bill should proceed until the outstanding concerns with the Assistance & Access Act have been addressed.

The Bill should be assessed against the potential to undermine the encryption of digital services. End-to-end encryption is a standard and essential tool used across the technology industry to protect the security of Internet users and their data. For many years, there has been an active debate in Australia about the impact of increased use of end-to-end encryption on law enforcement. DIGI's members are committed to working with policymakers and law enforcement to keep Australians safe; however there was widespread opposition from the broader technology industry in response to the Assistance & Access Act about legislative measures that undermine the effectiveness of end-to-end encryption. We reiterate the concerns DIGI has made in relation to the Assistance & Access Act in various submissions, and many of the concerns raised by the broader technology industry could apply to the Bill in question.

Lack of privacy protections

The warrants under this Bill may serve to compromise the privacy of users of the service provider's digital products, and it is unclear how law enforcement will mitigate against the violation of users' privacy rights. It is important to note that when account takeovers occur, law enforcement has access to *all* content and data, not just the content and data needed to complete the investigation. This is why it is imperative that there be rules in place for minimising the collection, retention, and use of data that is not relevant to the investigation.

While we welcome the fact that the Bill proposes that magistrates must have regard to the impact on privacy in determining whether to issue an Account Takeover Warrant, this limited and vague safeguard for privacy is not sufficient. The Bill does not involve any consideration of privacy in determining whether to issue Data Disruption Warrants, Network Activity Warrants nor in determining whether to issue an emergency authorisation in relation to account takeover warrants. As well as examining whether these warrants are *proportionate*, conventional human rights-respective approaches would also examine *necessity*. There needs to be far stronger protections for privacy across all of the warrants contemplated in the legislation, and these protections need to be reflected in consistent documentation and processes in the issuance of these warrants.

In light of the privacy and security concerns noted above, law enforcement bodies should have a standard framework for a documented Privacy Impact Assessment that they document for every warrant issued under the Bill. To "have regard to" privacy in issuing account takeover warrants (the wording used in Bill) is highly general language, and does not require a high or specific standard of privacy or data protection considerations, nor is it a replicable or consistent process for agencies to follow each time an order is issued. This Privacy Impact Assessment, or other such framework, should consider:

1. The necessity of the information being requested, and the need to minimise the collection of personal information to what is strictly necessary.
2. Whether the proposed method of accessing the information is the least privacy-infringing method available.
3. Whether the infringement on privacy is proportionate to the harm that will be averted by granting law enforcement access to the information.
4. An explicit requirement that agencies must show that they have attempted all other means of information access that would have a lesser privacy impact on individuals, and provide an explanation of why these alternate means are insufficient.
5. Requirements to minimise the retention of the data accessed during the investigation to a limited, specified period of time.

The explanatory memorandum alludes to such considerations at [24] and claims that they are mandatory, however there is no actual requirement under the Bill for the issuing authority to consider these issues. The privacy considerations listed above need to be reflected in the Bill itself.

As a default, the legislation should require transparency for end users affected, unless such transparency would compromise the aims of investigation. It is concerning that the Bill does not have

any provisions for agencies to notify end users of requests where possible, nor does it offer an avenue for challenging the need for access, nor does it clarify the rights of providers in relation to such notice. In fact, it may be an offence to notify users of the existence of these warrants, even once they are expired. Service providers should have explicit rights to meet community expectations in relation to notice; the Electronic Frontier Foundation has for many years published annual report on technology companies' handling of government surveillance requests in line with consumer expectations, and it specifically recognises companies that inform users about government data requests, while also recognising there are types of investigations that preclude advance notice.[1]

Introducing a Privacy Impact Assessment, or other comparable measures to protect user privacy, would serve three important goals:

1. They would be in line with consumer expectation of their data privacy. The Australian Government recognises that data privacy and protection are of importance to Australians, as this is the foundation for its current review of the Privacy Act 1988.
2. It would provide necessary reassurances to the service provider on the due diligence undertaken, and necessity of warrants supplied under the Bill.
3. They would also ensure that the Bill provides the expected protections for privacy to assist Australia's efforts to be a qualifying foreign power under the CLOUD Act, discussed later in this submission.

Lack of procedural fairness

If service providers are caught by this Bill, there should be an opportunity for them to challenge the issuance of a warrant or assistance order under the Bill. While we understand the need for law enforcement to be able to move swiftly in their investigations, there should be due process and procedural fairness for situations where service providers object to the warrant or particular elements of it. Under the current drafting of the Bill, there is very limited opportunity for a service provider to object to the issuance or execution of a warrant or an assistance order. Further guidance on this should be enshrined in the final legislation, and should incorporate meaningful guidance on:

1. the grounds on which a provider can object to the issuance of a warrant or an assistance (e.g. conflict of laws or technical inability);
1. to whom a provider should address an an objection;
2. the body that would be charged with independently reviewing the objection;
3. the timeframe for objections;
4. the legal status of providers after an objection has been lodged;
5. an indication of the assessment criteria for how such objections will be approved or denied.

Lack of interoperability with the CLOUD Act

We understand that the Account Takeover Warrant will apply extraterritorially with law enforcement being authorised to take control of an online account, regardless of where the account data is located. Similarly, Network Activity Warrants and Data Disruption Warrants can be issued in respect of computers located in foreign countries.

DIGI strongly supports the efforts being made by the Australian Government to enter into an agreement with the US Government for access to electronic communications under the US enacted Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The CLOUD Act enables companies to disclose data to law enforcement subject to an appropriate consenting official being satisfied about the maintenance of robust procedural protections for privacy and human rights.

The US Department of Justice has emphasised the importance of privacy in Designated International Agreements under the CLOUD Act with foreign partners:

[1] Electronic Frontier Foundation (2017), *Who Has Your Back? Government Data Requests 2017*, accessed at https://www.eff.org/who-has-your-back-2017

> *"The Act permits our foreign partners that have robust protections for privacy and civil liberties to enter into executive agreements with the United States to use their own legal authorities to access electronic evidence in order to fight serious crime and terrorism. The CLOUD Act thus represents a new paradigm: an efficient, privacy-protective approach to public safety by enhancing effective access to electronic data under existing legal authorities. This approach makes both the United States and its partners safer while maintaining high levels of protection of privacy and civil liberties*[2]*".*

It is also important to clarify that the CLOUD Act does not expand the powers of the US Government to issue search warrants to US service providers, nor does it modify or relax the high standards that the US Government must meet to obtain a search warrant. These high standards under US law must be reflected in this Bill and other emerging Australian Bills, such as the *Telecommunications Legislation Amendment Bill 2020* (International Production Orders). Otherwise, there is a risk of Australian law diverging from the robust protections for privacy and civil liberties required to enter into a CLOUD Act agreement under US law.

Additionally, it is important to clarify that the CLOUD Act does not create any new form of warrant; it simply removes the prohibition for providers under the US Stored Communications Act that prevents American providers from sharing data in direct response to requests from qualified foreign governments, and clarifies their obligations to disclose information pursuant to US warrants[3]. In contrast, the Australian Bill attempts to create three new types of warrants -- in addition to existing orders under the Assistance & Access legislation and the proposed International Production Orders Bill -- with which providers must understand their legal obligations and comply, without a clear objections process, as detailed earlier.

Potential conflict of laws

The Bill raises a number of conflicts of law issues for overseas service providers, particularly those located in the United States. All three warrants created by the Bill have the potential to create conflicts with laws in the United States, including the Stored Communications Act, the Wiretap Act and the Computer Fraud and Abuse Act. Additionally, the warrants contemplated under this Bill potentially raise conflicts with the United States Constitution, specifically the Fourth Amendment and the requirement that requires the US government to establish a particularised probable cause finding for each person or place to be searched. However, there is no express exception in the Bill for a service provider to refuse to comply with a warrant on the basis of these overseas laws; this puts overseas service providers in an untenable position to choose between violating Australian law and laws in other jurisdictions, giving rise to potential civil and criminal liabilities. Further consideration needs to be given to the interaction between this Bill and foreign laws.

Scope of services is overbroad

Building on the point above, in relation to the interoperability of the Bill with overseas laws, the Bill's scope extends beyond the standards of the US' Stored Communications Act which is limited to companies such as email providers, cell phone companies, social media platforms, and cloud storage services. The US Department of Justice has specifically clarified that "they do not include a company just because it has some interaction with the Internet, such as certain e-commerce sites"[4].

The overbroad scope of the Bill therefore creates uncertainty for enterprise and B2B companies. Furthermore, the Bill includes provisions under which law enforcement can compel specified persons

---

[2] US Department of Justice (2019) *FAQ, Promoting Public Safety, Privacy, and the Rule of Law Around the World,* available at: https://www.justice.gov/dag/page/file/1153466/download
[3]US Department of Justice (2019) *FAQ, Promoting Public Safety, Privacy, and the Rule of Law Around the World,* available at: https://www.justice.gov/dag/page/file/1153466/download
[4] US Department of Justice (2019) *FAQ, Promoting Public Safety, Privacy, and the Rule of Law Around the World,* available at: https://www.justice.gov/dag/page/file/1153466/download

to provide reasonable information and assistance to help them carry out a warrant (*Surveillance Devices Act* ss 64A and 64B(1), *Crimes Act* s 3ZZVG). It is possible that the assistance provisions in the Bill could capture digital companies that are providers of services to a third party, particularly enterprise and B2B services. For example, a business customer may be the target of one of these warrants, but the warrant could be served to the hosting technology platform provider. Further clarification of the term 'specified person' in the legislation is needed, to prevent such a predicament.

We also have concerns with the breadth of users that could be captured by a Network Activity Warrant. The definition of an "electronically linked group of individuals" is so broad as to potentially cast the net over a very large group of users who have no reasonable relationship with a suspect. Greater clarity and limits should be provided to protect the privacy of individuals without a reasonable link with the person in question.

Lack of prior judicial authorisation

The Bill proposes that Account Takeover Warrants are to be issued by a magistrate, and Data Disruption and Network Activity Warrants can be issued by an eligible judge or a nominated member of the Australian Appeals Tribunal (AAT).

In the past, DIGI has registered concerns about the Assistance & Access Act's lack of prior judicial review in the issuing of Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs). DIGI, along with many other industry associations, has argued that the far-reaching powers granted by the Act must be supervised by an eligible judge for sufficient prior oversight and independence. It is important to note that the Bill in question also does not provide prior judicial review under a robust legal standard.

This is not just an important point to industry, but has been important in the past to the US Congress, as any Designated International Agreement between Australia and the US under the CLOUD Act would have to comply with the robust certification requirements outlined in the CLOUD Act, or risk disapproval by the US Congress.

In a letter dated October 4 2019, the US House Judiciary Committee raised concerns to the Australian Government in relation to the Assistance & Access Legislation, highlighting that its lack of privacy protections may preclude an Designated International Agreement under the CLOUD Act. The letter specifically expresses concerns that the Assistance & Access Legislation does not require independent judicial review before or after the government issues an order requesting content from private businesses[5]. It is reasonable to deduct that these same concerns may hold in relation to the Bill in question.

While the Bill does allow for review of law enforcement demands by either a judge or a nominated Administrative Appeals Tribunal (AAT) member, it is important to note that Tribunal is not a court and falls under the portfolio of the Attorney General. There should be more independent oversight over decisions to counterbalance the Ministerial discretion currently reflected in the Bill.

We note that the Senate Standing Committee for the Scrutiny of Bills has equally highlighted this point in its recent Scrutiny Digest 1/21, 29 January 2021:

> *"The committee has had a long-standing preference that the power to issue warrants authorising the use of coercive or intrusive powers should only be conferred on judicial officers. In light of the extensive personal information that could be covertly accessed, copied, modified or deleted from an individual's computer or device, the committee would expect a detailed justification to be given as to the appropriateness of conferring such powers on AAT members, particularly part-time senior members and general members. In this instance, the*

[5] Hunter, F., (8/10/2019), "Deal to access US data for law enforcement at risk over controversial Australian law" in Sydney Morning Herald, accessed at https://www.smh.com.au/politics/federal/way-of-the-future-australia-and-us-negotiating-access-to-law-enforcement-data-20191008-p52ynm.html

explanatory memorandum provides no such justification."[6]

Low threshold of criminal offenses

The Bill has been publicly positioned as enabling law enforcement to have greater powers to address terrorism, child abuse and human trafficking. These are incredibly serious offences and companies have extensive processes in place to rapidly and routinely cooperate with law enforcement over such investigations. However, the Bill is drafted such that it can be applied to preventing or investigating criminal offences that carry a prison sentence of three years. This is far below the sentencing of such crimes.

We therefore strongly recommend raising the threshold for offences which could give rise to the powers of the Act being used. The Telecommunications (Interception and Access) Act 1979 (TIAA) already contains a definition of 'serious offence' in Section 5D.

DIGI raised the same issue above in a joint submission with the Communications Alliance and other industry associations in relation to the Assistance & Access Act. These concerns were reflected in the INSLM report reviewing that Act, released in July 2020, where Dr Renwick recommended that the threshold for the offence be raised to 'serious offence' in line with the offence threshold of the Telecommunications (Interception and Access) Act 1979.

[6]Scrutiny Digest 1/21, 29 January 202, Senate Standing Committee for the Scrutiny of Bills, p.30