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

Thursday April 30, 2020

Dear Committee Secretary,

Thank you for the opportunity to provide input on the Telecommunications Legislation Amendment (International Production Orders) 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 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.

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 the US enacted Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The CLOUD Act enables companies to provide information to law enforcement while maintaining robust procedural protections for privacy and civil liberties. The Bill is a step towards the US Government entering into a Designated International Agreements (otherwise known as an "executive agreement") with Australia, and we broadly welcome developments that move Australia towards such an agreement in relation to the CLOUD Act.

That said, we have concerns that the Bill lacks the robust procedural protections for privacy and civil liberties that Australians and the technology industry would expect. In saying that, it is 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 must be reflected in the Bill and in Australia's Designated International Agreement. Currently, there is a divergence between what the CLOUD Act makes mandatory under US law and what the Bill makes mandatory under Australian law; therefore we argue that the Bill overreaches in pursuit of what is necessary for an Designated International Agreement. In this submission, we will elaborate on these high level concerns in relation to particular omissions and additions in the Bill.

We acknowledge that the consultation for this Bill is happening at a time of unprecedented health and economic challenges due to the COVID-19 global pandemic. We encourage the Committee to ensure that robust consultation is not overlooked, and that the Bill is not rushed as a result.

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)

The Bill's mandatory obligations go beyond standards in the CLOUD Act

The Bill attempts to create a mandatory enforcement mechanism with civil and criminal penalties and this is fundamentally different to the US CLOUD Act. Additionally, the CLOUD Act does not create any new form of warrant. It simply clarifies the obligations for providers under the US Stored Communications Act, including their obligations to disclose information pursuant to US warrants[1]. In contrast, the Australian Bill attempts to create a new type of order -- in addition to existing orders under the Assistance & Access legislation -- with which providers must understand their legal obligations and comply, without a clear objections process, as detailed below. The CLOUD Act also does not permit indiscriminate or bulk data collection[2], while the Australian Bill again lacks such protections.

Finally, the Bill's enforcement threshold that "one or more Australians have posted material on a general electronic content service provided by a designated communications provider"[3] also 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

[1]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
[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] P.141 of the Bill

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 Bill lacks prior judicial authorisation

In the past, DIGI has registered concerns about the Assistance & Access legislation'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 representing the technology industry, has argued in relation to this legislation that the far-reaching powers granted by the legislation must be supervised by an eligible judge for sufficient prior oversight and independence. It is important to note that the Bill in question, pertaining to International Production Orders (IPOs), also does not provide prior judicial review under a robust legal standard.

This is not just an important point to industry, but has 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. As a related aside, we would echo the call from the Senate Standing Committee For The Scrutiny Of Bills that the Designated International Agreement also be tabled in Australian Parliament[5]. The CLOUD Act requires non-US government requests for criminal evidence to "to be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order." 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[6]. 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.

Finally, the fact that the Assistance & Access legislation lacks the condition of prior judicial review should not be used to extend the same standard to other emerging legislation. That legislation is currently under review by the Independent National Security Legislation Monitor and, as noted, this element of the legislation has been contentious to the technology industry and to the US House Judiciary Committee. Furthermore, the Senate Standing Committee For The Scrutiny Of Bills has specifically indicated that troubling precedents in existing legislation should not be used to justify a lack of prior judicial review:

> *The committee has a long-standing scrutiny view that the power to issue warrants or orders relating to the use of intrusive powers should only be conferred on judicial officers. In this*

[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
[5] The Senate (2020), *Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2020*, available at https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2020/PDF/d05.pdf?la=en&hash=59FE28DE5D0650BA01AA443EB52D0DF8B27BA103, p. 35
[6] 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

regard, the committee does not consider that consistency with existing provisions is, of itself, a sufficient justification for allowing warrants or orders relating to the use of intrusive powers to be issued by non-judicial officers.[7]

The Bill lacks privacy protections

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

> *"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*[8]*".*

The Bill lacks these robust protections for privacy, yet we note and welcome the fact that the Bill states:

> *In deciding whether to issue an international production order under subclause (2), the issuing authority must have regard to the following matters:*
>
> *(a) how much the privacy of any person or persons would be likely to be interfered with by the criminal law enforcement agency obtaining, under an international production order, a copy of the stored communications;*
> …
> *(d) to what extent methods of investigating the serious category 1 offence or serious category 1 offences that do not involve so disclosing the telecommunications data have been used by, or are available to, the enforcement agency;*

However, these commitments need to be accompanied by more robust documentation and processes. There should be a standard framework for a documented Privacy Impact Assessment that should be documented for every IPO issued. This assessment should include a framework to assess the proportionality where the negative privacy impact is assessed against the benefits of the personal information access. "Have regard to", the language used in (a) above, does not require a high 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 assessment should consider the necessity of the information being requested, building upon (d) above, minimising the collection of personal information to what is strictly necessary. In this regard, there should be an explicit requirement for agencies to consider other means of information access that have a lesser privacy impact on individuals and provide an explanation of whether these alternate means have been tried and how they have failed.

---

[7]The Senate (2020), *Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2020*, available at https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2020/PDF/d05.pdf?la=en&hash=59FE28DE5D0650BA01AA443EB52D0DF8B27BA103, p. 26

[8] 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

Furthermore, there should also be transparency to end users affected, where such transparency does not 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, and does not clarify the rights of providers in relation to such notice. 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.[9]

Introducing such measures in relation to privacy and data protection would service several important goals: they would be in line with consumer expectation of their data privacy, provide necessary reassurances to industry on the diligence behind and necessity of IPOs, and ensure that the Bill provides the expected protections for privacy to serve as a foundation an Designated International Agreement to be a qualifying foreign power under the CLOUD Act. It would also serve to allay concerns raised by the Senate Standing Committee For The Scrutiny Of Bills as noted below:

> *"The committee notes that the framework the bill seeks to establish could significantly trespass on a person's rights and liberties and considers that the inclusion of such provisions should be sufficiently justified and that appropriate safeguards should be in place to ensure that a person's electronic information and communications data is only accessed in appropriate circumstances."*[10]

The Bill lacks a process for providers' objections

We welcome the Bill's provision to allow providers to object to IPOs under Part 7, and seek further operational detail as to how objections should be carried out procedurally. This further guidance should be enshrined in the final legislation, and should incorporate meaningful guidance on:

I. who a provider should address an an objection to;
II. the body that would be charged with independently reviewing the objection;
III. the timeframe for objections;
IV. the legal status of providers after an objection has been lodged in relation to the IPO;
V. an indication of the assessment criteria for how such objections will be approved or denied.

In addition, it is concerning that the Bill only allows providers to "object to the order on the grounds that the order does not comply with the designated international agreement nominated in the application for the order."[11] Providers are not currently privy to the contents of Australia's forthcoming Designated International Agreements and, as noted, these agreements are not even currently required to be tabled in Australian Parliament. If criteria is to be provided for the grounds upon which an objection can be made, it should be specified within the Bill. The Bill, as currently drafted, generally lacks meaningful guidance on the objection process. Without this clarified in the legislation, it becomes a high legal risk undertaking for any provider to issue such an objection.

Telephone orders must be accompanied by written orders

It is concerning that the Bill appears to allow agencies to make an application for an IPO by telephone. It is unclear in the Bill's language whether this allows the agency to serve the IPO to a

[9] Electronic Frontier Foundation (2017), *Who Has Your Back? Government Data Requests 2017*, accessed at https://www.eff.org/who-has-your-back-2017
[10] The Senate (2020), *Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2020*, available at https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2020/PDF/d05.pdf?la=en&hash=59FE28DE5D0650BA01AA443EB52D0DF8B27BA103, p. 25
[11] p. 138 of the Bill

provider by telephone, which would be highly problematic for the reasons outlined below -- if this is not the case, it ought to be made explicit in the legislation.

In any case, the standard outlined for a telephone application is highly discretionary:

> *(2) However, a person making the application on the enforcement agency's behalf may make the application by telephone if the person:*
>
> *(a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subclause (3); and*
>
> *(b) thinks it necessary, because of urgent circumstances, to make the application by telephone.*[12]

Should this extend to the delivery of IPOs to service providers, while we recognise that there may be highly urgent exceptional investigations where a telephone call may be appropriate, a telephone call should simply serve as a "heads up" advance notice of an urgent IPO to enable the provider to commence their preparations to respond to a request. It is simply unacceptable that any order may be made by telephone only; every request must be made in writing, even if a telephone call is used in the first instance, and the written order needs to be sent within a specified window of the initial phone call. This documentation is vitally important for i) the providers' accuracy in responding to the request ii) in legally protecting the provider and iii) in the interests of transparency.

It is also worth highlighting that many companies have processes in place to expeditiously consider law enforcement requests for access to information in an emergency. These currently operate effectively and are conducted in writing.

The sharing of user information with law enforcement is not a situation that should be taken lightly and is an issue of importance to Internet consumers, necessitating the need for robust documentation in every step and every instance where this has taken place. This documentation should exist even in circumstances where the provider is explicitly legally prohibited from disclosing the order, because doing so may compromise the investigation, so that it can be reviewed at a later stage.

Standards for incoming orders from a foreign countries

While we have focused the bulk of this submission on factors that we consider will enable reciprocity with CLOUD Act, as most of DIGI's members are US-headquartered providers, we also encourage further attention in the final Bill and all Designated International Agreements to ensuring that they do not enable the misuse of data in all foreign countries. We would echo the concerns raised by the Senate Standing Committee For The Scrutiny Of Bills that:

> "... the provisions as currently drafted have the potential to significantly trespass on a person's rights and liberties, particularly in circumstances where access to information held in Australia may be given to foreign jurisdictions whose governance structures are not underpinned by respect for the rule of law and the separation of powers."[13]

[12] p. 49 of the Bill.
[13] The Senate (2020), *Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2020*, available at https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2020/PDF/d05.pdf?la=en&hash=59FE28DE5D0650BA01AA443EB52D0DF8B27BA103, p. 64