30 April 2020

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
By online submission

TELECOMMUNICATIONS LEGISLATION AMENDMENT (INTERNATIONAL PRODUCTION ORDERS) BILL 2020– BSA COMMENTS

BSA | The Software Alliance (BSA) is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[1] are among the world's most innovative companies, creating software solutions that spark the economy.

BSA and our members have an interest in the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (Bill) currently being reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). As stated publicly, we understand that the Bill intends to provide for the legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic information and communications data, such as that being negotiated with the United States for the purposes of the US *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*.[2]

Executive Summary

BSA acknowledges and supports the Australian Government's desire to have more powerful tools to aid in the fight against criminal and terrorist activity and to ensure that the rule of law applies equally to online and offline activity.

As the Government considers new legislation to expand surveillance powers, BSA encourages close collaboration between the Government, Australian law enforcement authorities, and the technology community to improve processes and methodologies enabling law enforcement access to digital evidence in a timely manner.

BSA notes that the Bill requires an underlying international agreement to enable it, and that Australia is currently negotiating an agreement with the United States for the purposes of the CLOUD Act. In light of that, it is important for the Australian Government to ensure that the Bill considers issues such as jurisdiction for applicability of IPOs and provides sufficient checks and balances to meet the requirements for an executive agreement with the United States under the CLOUD Act.

[1] *BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.*

[2] https://www.congress.gov/bill/115th-congress/house-bill/4943

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

To ensure successful implementation of the Bill, BSA suggests the following amendments be consider by the Committee:

1. The issuance of International Production Orders (IPOs) should be made by an independent judicial authority based on evidence from the requesting interception agency regarding the necessity of issuing the IPO including why other less intrusive measures are unavailable or insufficient, as well as the reasonableness, proportionality, practicability, and feasibility of the proposed requirements.

2. The Bill should require that designated communications providers (Provider) be consulted prior to issuance of an IPO.

3. The Bill should allow for a Provider to challenge an IPO before an independent judicial authority on the grounds that the request is technically infeasible, not practicable, or otherwise impossible to comply with including when there is a conflict of international law. Furthermore, such an appeal should suspend the requirement for the Provider to comply with the IPO for the duration of the appeal.

4. The scope of application of the Bill should be narrowed to the prevention, detection, investigation or prosecution of serious offences, defined as offences punishable by 7 years or more of imprisonment.

5. BSA recommends that the Bill clarify whether the Bill is intended to only access Australian-sourced data. If so, BSA recommends that Providers also be given the ability to appeal against the issuance of an IPO on the basis that the requested information is not Australian-sourced.

6. The Bill should clarify how IPOs apply to subsidiaries and other legal entities and ownership structures to avoid unintended consequences such as accessing data from jurisdictions with which Australian has no designated international agreement.

7. The Bill should provide that the manner of implementing an interception or information access requirement under an IPO be arrived at through mutual consultation between the Provider and the interception agency.

General Comments

BSA's members have worked closely with law enforcement in Australia, the United States, the United Kingdom, and elsewhere around the world to ensure that law enforcement authorities can access digital evidence in support of lawful criminal investigations in a timely manner pursuant to appropriate safeguards. For law enforcement authorities to take advantage of the opportunities new technologies bring, and to overcome the array of associated challenges, digital evidence access must be approached collaboratively. In this regard, the Bill must serve as a platform to facilitate and deepen collaboration between the technology and law enforcement communities by establishing the foundation of a constructive partnership that takes into account the priorities, needs, and sensitivities of all relevant stakeholders.

The needs of law enforcement authorities, technology providers, and the consumers whose privacy and security interests are at stake are best met by policies and laws that provide for robust mechanisms for judicial oversight, transparency of activities, privacy and security protections, and clearly defined processes for bi-directional communication on law enforcement needs. In addition, as data is stored by global organizations subject to laws in different countries, it is increasingly important that laws for government access be internationally interoperable.

BSA strongly urges continued dialogue between the Australian Government, policymakers, and industry to find solutions that balance the legitimate rights, needs, and responsibilities of the

Government, citizens, providers of critical infrastructure, third party stewards of data, and innovators. We would also welcome the opportunity to speak with the PJCIS at any hearing it holds.

Specific Comments and Suggested Amendments

In addition to our general comments above on the policy and global regulatory environment, BSA offers in this section our specific comments and recommendations on the Bill:

1. The issuance of IPOs should be underpinned by independent judicial oversight

The Bill as written allows for different issuing authorities depending on the purpose of the IPO. In criminal cases and control orders, a judicial officer, or a senior member of the Administrative Appeals Tribunal (AAT), can issue an IPO. In the case of national security, only a member of the AAT Security Division may issue an IPO.

The US CLOUD Act §2523(b)(3)(D)(v) requires that orders issued by a foreign government be subject to review or oversight by a court, judge, magistrate, or other independent authority.

We are concerned that the AAT may not be seen as sufficiently independent in the IPO issuance process to ensure public and overseas government trust. Fundamentally, as a part of the executive branch of the Australian Government, may not be seen as sufficiently independent to appropriately oversee the issuance of IPOs. At worst, it could be seen by the Australian public and overseas governments as the executive branch of the Australian Government approving its own applications for IPOs.

The circumstances relating to the issuance of any IPO could be very complex and could extend beyond the immediate merits of the application. Judicial authorities are generally considered to be best placed to weigh evidence presented from the requesting interception agency regarding the necessity of issuing the IPO including evidence as to why other less intrusive measures are unavailable or insufficient in the circumstances, along with other important considerations such as the reasonableness, proportionality, practicability, and feasibility of the proposed requirements.

Importantly, involving the Australian judicial system in the process of issuing of IPOs is a visible way of demonstrating that the powers of the executive branch are balanced in the Australia IPO regime. It would engender public trust in the process and legality of IPOs and provide assurance that the legal telecommunications intercept regime in Australia does not infringe on the rights of law-abiding Australians or investors doing business in or with Australia. Strong judicial oversight will help to give confidence to decision makers and potential signatories to designated international agreements that Australia has a robust and fair legal intercept and access regime.

Recommendation 1

BSA recommends that the issuance of an IPO should be made by an independent judicial authority based on evidence from the requesting interception agency regarding the necessity of issuing the IPO including why other less intrusive measures are unavailable or insufficient, and the reasonableness, proportionality, practicability, and feasibility of the proposed requirements.

2. Strengthen the IPO Issuing Process

As written, the proposed process in the Bill for the issuance of IPOs could allow IPOs to be given to Providers that are unable to be complied with or are impractical or infeasible in some way leading to ineffective or impossible compliance. BSA proposes the addition of a consultation and appeal steps to the IPO issuing process proposed under the current Bill. This will strengthen the process, and increase trust in the IPO regime ultimately providing for a more successful program.

Getting IPO requests right from the beginning is important as the issuance of flawed IPOs can lead to a loss of investigative time as the Provider explains to the interception agency any problems or issues

in complying with a particular request, potentially having to do so via the Australian Designated Authority (ADA). This could require multiple iterations backwards and forwards and be extremely wasteful in the event of a time-critical investigation.

This is a critical issue for Providers as it appears that an IPO remains in force even if there is an objection by the Provider, forcing them to comply with it until it is cancelled or face civil penalties under Part 8 of proposed new Schedule 1 to the *Telecommunications (Intercept and Access) Act 1979* (TIA Act) despite any legitimate concerns. This in turn means that, in theory, by the time the ADA comes to a decision on the IPO, the damage could already have been done (and the interception carried out or the information handed over) by Providers who wish to avoid civil penalties.

Pre-issuance consultation with providers

The affected Provider currently has no right to comment on the IPO until after it has been issued and given to the Provider by the ADA. It is critical for the success of the IPO regime that the Provider is consulted prior to the issuance of an IPO.

This is a significant weakness in the process. Without consulting with the Provider, it is highly possible to issue an IPO that is neither practicable nor feasible to comply with. The interception agency, ADA, and issuing authority are not in a position to assess the technical merits of a request. The only entity with the engineering and technical information needed to perform that assessment is the Provider itself. In addition, the Provider is the only entity capable of assessing whether it has the data in its systems, or even if the telecommunications identifiers available to the interception agency are sufficient to find the data in the Provider's systems.

The Provider is also the only entity likely to know the location of the data or the legal obligations of the legal body able to access the data. It is therefore the only entity able to assess whether they would be prevented from complying due to an international conflict of laws as a result of the location of the data. Potentially, the data requested could in part be held in Australia and therefore be accessible using existing interception powers.

Further, while the Bill provides that certain matters must be taken into consideration regarding an IPO, the cost or impact on the Provider is not a matter to be considered. BSA is concerned that, without taking cost and impact on the Provider into consideration, complying with an IPO or a series of IPOs could be to the significantly detriment of the Provider in question, for which the Provider could have no means to seek compensation or relief.

BSA strongly believe that by ensuring that the Provider is consulted prior to the issuance of an IPO would greatly reduce the amount of investigative time wated in the issuance of impracticable or infeasible IPOs that are unable to be complied with. The Bill does not contain any obligation for the Provider to be consulted at any stage in the process.

Right of full appeal for providers

Under the current process, Providers are only able to object to an IPO by writing to the ADA. This is a particularly important concern in this case where there is a high potential for Providers to be exposed to conflicts of law. However, an appeal is only allowed on the grounds that the IPO is inconsistent with the designated international agreement. It is unclear how this request for review would be handled and what factors will be considered. The Bill also does not specify whether the ADA needs to seek input from the stakeholders or the timeframe for the ADA to come to a decision.

BSA notes again that it is unclear whether this appeal would suspend a Provider's obligation to comply with the IPO which would already be in effect. As written the Bill could expose a Provider to civil liabilities for non-compliance if it appeals an IPO issued to it and does not concurrently take steps to comply with the IPO, despite its legitimate concerns with compliance.

BSA suggests that in order to rectify these concerns Providers should have the opportunity to challenge a proposed IPO before an independent judicial authority based on factors relating to feasibility, legality, practicability, and international comity. Additionally, it is suggested that the requirement to comply with the IPO should be suspended and any enforcement proceeding for non-

compliance with the IPO that would otherwise be applied should be prohibited or stayed pending any appeal process.

Should the Australian government nonetheless decide to continue to confer the power on the executive branch to issue IPOs, then we recommend that there should be a mechanism to allow for appeals to be made against executive decisions to issue IPOs on the merits of the case, or at the minimum by way of judicial review. In respect of the latter, we further recommend that the exclusion of the TIA Act from the application of the *Administrative Decisions (Judicial Review) Act 1977* (ADJRA) should be removed in respect of decisions to issue IPOs (so that the ADJRA will apply in respect of such decisions).

Recommendation 2

BSA recommends that the Bill make clear that Providers are to be consulted prior to issue of an IPO.

Recommendation 3

BSA recommends that the Bill allow for a Provider to challenge an IPO before an independent judicial authority on the grounds that the request is technically infeasible, not practicable, or otherwise impossible to comply with including when there is a conflict of international law. Furthermore, such an appeal should suspend the requirement for the Provider to comply with the IPO for the duration of the appeal.

3. Limit Scope of Applications

The Bill currently allows the issuance of IPOs for an unduly broad range of purposes. BSA is concerned that the broad scope of circumstances in which the powers can be exercised is overly broad and should be limited to the prevention, detection, investigation, or prosecution of serious offences. To bring it in line with existing provisions in the TIA Act, serious offences should be limited to offences punishable by 7 years or more of imprisonment. The lesser 'category 1 serious offences' allowed for in some cases in the Bill should be removed.

Under the US CLOUD Act §2523(b)(3)(D)(i) the purpose for which a foreign government can issue an order is restricted to the prevention, detection, investigation or prosecution of serious crime, including terrorism. National security as a purpose for issuing IPOs is not further defined by the Bill but if it is taken as the definition given by the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018[3] would include purposes that would fall outside of the CLOUD Act limitation.[4]

Recommendation 4

BSA recommends that the scope of application of the Bill be narrowed to the prevention, detection, investigation, or prosecution of serious offences, defined as offences punishable by 7 years or more of imprisonment.

4. Strengthen safeguards and clarify operation

The Bill describes a complex system of designated international agreements and warrants issued on Providers. The Explanatory Memorandum notes that the Bill will 'introduce a regime for Australian agencies to obtain independently-authorised international production orders for interception, stored communications and telecommunications data directly to designated communications providers in

[3] https://www.legislation.gov.au/Details/C2018C00506

[4] The National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 defines in section 90.4 the national security of Australia as:

a) the defence of the country;

b) the protection of the country or any part of it, or the people of the country or any part of it, from espionage, sabotage, terrorism, political violence, interference with the defence force, and foreign interference;

c) the protection of the integrity of the country's territory and borders from serious threats;

d) the carrying out of the country's responsibilities to any other country in relation to (b) and (c); and

e) the country's political, military or economic relations with another country or other countries.

foreign countries with which Australia has a designated international agreement'. BSA is concerned that, as written, the Bill could allow for unintended use of the IPO powers beyond the stated intent and introduce unexpected legal complexity with respect to the origin and location of data, and different Provider corporate structures.

No limitation on origin of data

Although it is noted in the Explanatory Memorandum for the Bill that data obtained through the powers in the Bill must be Australian-sourced, the Bill itself does not clearly specify this as a limitation. Australian-sourced data is defined in the Bill in section 3(8) but it is not clear in the Bill that data requested under an IPO must be Australian-sourced and that seeking data that is not Australian-sourced is a reason to deny an application.

Recommendation 5

BSA recommends that the Bill clarify whether the Bill is intended to only access Australian-sourced data. If so, BSA recommends that Providers also be given the ability to appeal against the issuance of an IPO on the basis that the requested information is not Australian-sourced.

No limitation on location of data and unclear treaty relationship

There seems to be no limitation on the location of data that is the target of an IPO, and no relationship between a designated international agreement and the location of the data. This seems to allow for situations whereby IPOs could be legally issued for purposes outside of the stated intent of the Bill.

There is an unclear relationship in the IPO application and issuance process between the designated international agreement and the location of the data sought by the IPO warrant. This could allow circumstances whereby an IPO could access data in a way that potentially circumvents the safeguard of having a designated international agreement in place with the country where the data is sourced.

> *Example 1 – Issuing an IPO for data held in a jurisdiction without an agreement with Australia*
> Company A is a multi-national company based in a country with a designated international agreement with Australia. It holds data of interest to interception agencies in servers in a third country that does not have a designated international agreement with Australia. As written, the Bill allows an IPO to be issued against Company A for the data held in the third country extending the reach of the Bill beyond the authorised international agreement, and raising potential conflict of laws and liability issues for Company A (the Provider).

Designated communications provider clarity

Another concern is that the Bill does not seem to consider subsidiaries and corporate entities as potential targets of IPOs. The Bill currently appears to allow the issuance of an IPO against any entity that meets the Provider definition and that has any legal presence inside a jurisdiction with a current international treaty with Australia. This could include subsidiaries and other legal entities and ownership structures, and could lead to a number of unintended consequences that appear to be at odds with the stated aim of the Bill. As in the previous example, this could lead to a situation where an IPO could access data held in a jurisdiction with does not have a designated international agreement with Australia.

> *Example 2 – Issuing an IPO for data held in a jurisdiction without an agreement with Australia*
> Company B is a multi-national company based in a country without a designated international agreement with Australia. Company B holds data of interest to Australian interception agencies. It has a wholly owned subsidiary, Company C that is incorporated in a country that does have a designated international agreement with Australia. As written, the Bill appears to allow an IPO to be issued against Company C for data held by Company B in a country that does not have a designated international agreement with Australia. Again, this extends the reach of the Bill beyond the authorised international agreement and raises potential conflict of laws and liability issues for Company B (the Provider).

Recommendation 6

BSA recommends that the Bill clarify how IPOs apply to subsidiaries and other legal entities and ownership structures to avoid authorizing unintended circumstances such as accessing data from jurisdictions with which Australia has no designated international agreement.

5. Remove the ability to determine manner of 'intercept'

The wide scope of the powers under the Bill, include wide latitude for law enforcement to determine the manner of implementing the interception and information access requested as noted in Section 31(4). However, when determining how an IPO is to be fulfilled, interception agencies are not in the best placed to decide how best to seek data within a Provider's system. To do so could unnecessarily impact Providers and cause unexpected delays as Providers are forced to use inefficient and ineffective methods to access data within their own systems.

Recommendation 7

BSA recommends that, in line with Recommendation 2 above, the Bill provide that the manner of implementing any interception or information access requirement under an IPO must be arrived at through mutual consultation between the Provider and the interception agency.

Conclusion and Next Steps

Given the complex nature of the Bill, the sensitivity of the subject matter and the numerous concerns highlighted above BSA suggests that the Committee consider the suggested amendments to the Bill. BSA and our members remain at the disposal of the Committee to further discuss the issues it has raised and the implications (and possible unintended consequences) of the Bill to ensure that the Australian Government is effectively able to address the challenges of accessing evidence in the digital age.

[redacted]

Yours faithfully,

[redacted]

Brian Fletcher
Director, Policy – APAC
BSA | The Software Alliance