



21 May 2020

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

TELECOMMUNICATIONS LEGISLATION AMENDMENT (INTERNATIONAL PRODUCTION ORDERS) BILL 2020

BSA QUESTIONS ON NOTICE

BSA | The Software Alliance (**BSA**)¹ again thanks the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) for the opportunity to testify on 13 May 2020. As a result of our testimony during the public hearing for the inquiry into the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (the **Bill**), we took several questions on notice that we would like to address.

As an overarching principle, we see that building collaborative relationships that recognize the equities of all stakeholders involved provides the most effective way to ensure sustainable, efficient mechanisms to access digital evidence in accordance with the law.

BSA's position on Mutual Legal Assistance Treaties

Cross border cooperation is necessary to enable Australian law enforcement agencies to access data, which is frequently stored in facilities dispersed around the world. From a designated communications provider (**Provider**) perspective, such cooperation provides mechanisms to reinforce procedural protections and legal safeguards.

Up until the passage of the US *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* in the United States, the practice of using mutual legal assistance treaties (**MLATs**) has been best practice in seeking digital evidence. BSA has long advocated for modernization the MLAT process by allowing electronic submission of requests and appropriate resourcing by the US Department of Justice's Office of International Cooperation. Law enforcement agencies and Providers share frustration with the speed and

¹ BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

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.

effectiveness of MLAT processes and recognize the need for a more efficient process for accessing digital evidence.

BSA supports CLOUD Act-based international agreements as the emerging best practice in solving some of the shortcomings of the MLAT system. Requests authorized by CLOUD Act-based agreements promise to be an inherently more efficient process for collecting digital evidence as they allow law enforcement agencies to make requests directly to data controllers. When done well they also ensure that individual privacy is protected, and rule of law is respected.

Examples of data not being able to be provided upon request due to technical reasons

BSA recommends that Providers be consulted before law enforcement entities issue an International Production Order (IPO). Including this step in the process for issuing an IPO will reduce the number of requests for digital evidence made that are inefficient or infeasible, and reduce the amount of time lost as a Provider reverts to the agency to repair the request. Also, as it is unclear whether a Provider could be exposed to civil liability under the Bill for non-compliance if it is unable to comply with an issued IPO, prior consultation would help mitigate this risk to Providers.

During our testimony, BSA was asked to provide specific examples of where a Provider may not be able to provide data in response to an IPO for technical reasons. As an industry association, we are unable to provide specific details of individual cases, but the examples below demonstrate some of the concerns of Providers with this particular aspect of the Bill.

Provision of appropriate identifiers to a Provider

Section 2 of the Bill defines a telecommunications identifier as the address or identifier used by the Provider to provide the communications service used by the subject of interest. It may be a telephone number, a unique identifier for a device, a user account identifier, an IP address, or an email address.

An IPO can be issued using a telecommunications identifier that is valid under the Bill but insufficient for a Provider to identify and recall individual carriage, message, or call application services of interest.

How data is accessed inside Providers' systems can vary widely depending on technology choices, business models, and individual user decisions. A Provider may issue users a unique customer number, self-selected username, unique device number, or cryptographic token to uniquely identify them within their system. Depending on the approach, the specific identifier needed to recall data related to a user will vary from Provider to Provider. On many services, including those providing messaging and voice calling services, common identifiers such as telephone numbers or IP addresses may not be a valid unique identifier to recall user data. To add further complexity, each Provider's technology is unique and what works as a valid unique identifier for a user in a Provider's system may not work for other Providers.

It is unlikely that a law enforcement agency would know exactly how Providers design their systems and what identifiers are used to uniquely identify individual users within the company's data holdings. As such, it may greatly increase the time needed to respond, or even be completely impossible for a Provider to recall the desired information if the law enforcement agencies requests data related to identifiers that are not sufficient to allow the Provider to respond.

Example

An IPO for a legitimate law enforcement investigation is issued to Provider A, requesting metadata associated with an identified telephone number. However, because of Provider A's technology choices and the ephemeral nature of some telephone numbers, it is not possible to discern the details of an individual user from those of other users that are not the subject of the investigation without further information (potentially location or time of use of the account), or alternative identifiers (like device ID or username).

A similar situation can arise due to compliance with some privacy regulations. Under the principle of minimization Providers are increasingly expected to collect as little information as possible to provide the requested service to a user. This means that some identifiers permitted under the Bill may not have been collected in the first place, and therefore would be insufficient to allow the Provider to respond. Only by consulting with Providers in advance will law enforcement authorities know what identifiers are collected and which are not.

Example

An IPO for a legitimate law enforcement investigation is issued to Provider B, requesting message content associated with an identified IP address. As Provider B practices the principle of data minimization, IP addresses associated with user activity are not collected and the Provider is therefore unable to respond to the request.

Seeking legally deleted data

Some jurisdictions require data to be deleted after it is no longer needed, or after a specific period of time. The most obvious international example of this legislation is the European Union's requirement to delete personal data under the General Data Protection Regulations (**GDPR**). Holders of personal data, which can include IP addresses, phone numbers, and other identifiers, are expected to actively manage their holdings, deleting data either because the purpose for collection has ended or at the request of the data subject.

Example



An IPO for a legitimate law enforcement investigation is issued to Provider C, requesting at-rest data associated with a specific user. As Provider C is subject to European law, they deleted the data when the user ceased to be a customer of the service. Provider C is therefore unable to respond to the request.

Using non-unique data in requests

Providers have reported fielding requests for digital evidence using non-unique data. This occurs when multiple users are assigned non-exclusive identifiers (e.g. when using VPNs, ephemeral phone numbers, or temporary identification numbers), when users are accessing common IP addresses or shared infrastructure, or when incomplete data is provided in requests (e.g. common names or partial names).

Example

An IPO for a legitimate law enforcement investigation is issued to Provider D, requesting at-rest data associated with a specific user and providing an IP address. Upon investigation, the Provider finds that the IP address belongs to common infrastructure, meaning that multiple users are associated with it in their user records. Provider D is then unable to answer the request without further information.

If you require any clarification or further information in respect of this submission, 


Yours faithfully,



Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance