April 30, 2020

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

RE: ACT | The App Association Comments Regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Dear Committee Secretary:

ACT | The App Association (App Association) appreciates the opportunity to provide input regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020. We understand the legislation has been proposed to set the framework for future bilateral comity agreements under the U.S. CLOUD Act (CLOUD Act), which would permit law enforcement in either country to obtain electronic evidence needed to investigate and prosecute crimes when that evidence is stored by providers based in the other country. Though the App Association continues to support the CLOUD Act framework and the creation of bilateral comity agreements in general, we oppose the legislation being considered here. The legislation would, without net public interest benefit, create overbroad authority to review and approve applications for international production orders; effectuate unacceptable extra-territorial enforcement powers; and produce unreasonable and infeasibly opaque challenge mechanisms for U.S.-based providers.

The App Association represents more than 5,000 app makers and connected device companies that create and support jobs in the United States and abroad. Our small and medium-sized member companies create innovative cloud-based solutions that improve workplace productivity, accelerate academic achievement, help people lead healthier lifestyles, and so much more. Every single one of these companies depends on the ability to access and transfer data, oftentimes across international borders to reach and serve customers overseas.

Although App Association members are small- to medium-sized enterprises (SMEs), they have clients and customers across Australia, key Australian trading partners, and the globe, and benefit significantly from the CLOUD Act's bilateral framework. Bilateral

agreements forged under the CLOUD Act remove barriers for companies doing business in multiple jurisdictions when a request for communications data from one government conflicts with the laws of the government where the data is stored or where the target of the investigation is from.

Unlike large multinational corporations, SMEs cannot afford lengthy battles with governments in court when they are forced to break one set of laws to comply with another. Yet, the App Association recognises that sovereign laws still must be respected, and the government's laws and rights created for their citizenry should follow their citizens wherever their data may be and wherever they may happen to be physically. As our member companies continue to serve an increasingly globalised society, bilateral agreements can ease some of the inevitable conflicts that arise between jurisdictions.

That said, bilateral comity agreements addressing law enforcement access to data are not an end in and of themselves; they are only desirable to the extent to which they respect the letter and spirit of the CLOUD Act, creating fair and reasonable standards for transparency and challenge that are reflected in the U.S. legal framework. Consequently, the App Association has several concerns with the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 as currently formulated, many of which were elucidated in a multi-stakeholder letter.[1] In this letter, the App Association provides its positions on problematic provisions in the proposed legislation and explains how such provisions will harm our small business members.

I. Overbroad Authority to Review International Production Orders

The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 introduces a regime for Australian agencies to obtain international production orders (IPO) for interception, stored communications, and telecommunications data directly from designated communications providers in foreign countries with which they have reached a bilateral agreement. The legislation would allow for eligible judges or nominated Administrative Appeals Tribunal (AAT) members to review and authorise law enforcement requests for each type of production order, subject to a set of "matters" those reviewers must consider prior to making their decision.

However, it is unclear whether this oversight mechanism satisfies conditions set forth in the CLOUD Act, which require that data requests stemming from foreign governments "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."[2] Nominated AAT members are not representatives of a court, judges, or magistrates, and are not

[1] Submission 9; https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IPOBill2020/Submissions

[2] United States CLOUD Act §2523 (b)(4)(D)(v); https://www.justice.gov/dag/page/file/1152896/download

independent authorities as that term is understood in the United States, since these individuals are appointed members of the executive branch.[3]

The App Association is concerned that expanding production order review authority beyond what is provided for in the CLOUD Act introduces unnecessary conflicts between U.S. and Australian law and opens the door for potential biases and abuses. As drafted, the legislation would require our members to respond to requests that did not honor judicial oversight standards enjoyed in the United States, forcing a decision as to which jurisdiction's laws it would violate. Such scenarios are harmful to the public interest and the data flows that power the global digital economy supporting countless Australian interests and businesses. We believe authorised production order reviewing authorities should be limited to those contemplated in the CLOUD Act and strongly recommend revisions to the legislation accordingly.

II. Extra-territorial Reach

The CLOUD Act removes the restrictions set forth in the Stored Communications Act to "allow them [U.S.-based providers] to respond to valid legal process sought by a governmental entity."[4] However, the legislation considered here would go further by asserting jurisdiction and imposing a new enforcement regime to penalise non-compliance. Part 8 of the legislation provides that "the designated communications provider must comply with the order to the extent to which the designated communications provider is capable of doing so" and attaches a civil penalty to entities who do not comply and meet the enforcement threshold. The App Association reiterates that similar enforcement regimes do not exist in other jurisdictions with which the United States has agreed to bilateral agreements under the CLOUD Act. As extra-territorial enforcement mechanisms are not supported by the CLOUD Act, and since such a measure violates emerging norms for bilateral agreements, the App Association requests that the PJCIS remove Part 8 of the legislation. Alternatively, Part 8 should be significantly modified to align with the CLOUD Act.

III. Opaque Challenging Mechanisms

The App Association is concerned that the legislation as currently written does not provide transparent and thorough mechanisms through which U.S.-based providers can clarify or challenge an order sought by an Australian agency. The only relevant mechanism detailed in the legislation can be found in Section 121, which simply states that providers who seek to object to an order "on the grounds that the order does not comply with the designated international agreement" must provide written notice to: "(a) be given to the Australian Designated Authority within a reasonable time after the international production order is given to the designated communications provider; and

[3] Administrative Appeals Tribunal Act 1975; https://www.aat.gov.au/about-the-aat
[4] United States CLOUD Act §2523 (b)(4)(I)(b); https://www.justice.gov/dag/page/file/1152896/download

(b) set out the reasons why the provider considers that the order does not comply with the designated international agreement nominated in the application for the order." The legislation provides no further information on how such challenges will be processed or assessed. The PJCIS should clarify and expand the procedures by which U.S.-based providers can obtain additional information and to challenge orders if they believe an order is vague, overbroad, or otherwise unlawful.

We thank the PJCIS in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,

Graham Dufault
Senior Director of Public Policy

Matt Schwartz
Innovators Network Foundation Privacy Fellowship Coordinator

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
[redacted]