April 24, 2020

RE: International Civil Liberties and Technology Coalition Comments Regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

To whom it may concern:

The undersigned organizations and companies jointly submit these comments regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020. We are an international coalition of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online, technology companies and trade associations, as well as technical and policy experts. We appreciate the opportunity to provide feedback on this important process, and to express our reservations about the bill as currently written. The draft legislation is designed to permit Australia to enter into a bilateral agreement with the United States under the U.S. CLOUD Act, thereby permitting each country to make direct requests for electronic communications information from providers based in the other country. While a number of undersigned organizations and companies are U.S.-based, we bring our experience and knowledge of the CLOUD Act in assessing the *International Production Orders* bill. We urge you not to move forward with the bill as currently written, because it does not provide adequate safeguards to protect human rights.

Members of this coalition have advocated extensively for rights-protective provisions in cross-border data sharing agreements, including in the implementation of the United States CLOUD Act. We urge the PJCIS that significant revisions to this bill are necessary for Australia to implement a framework that provides protections for privacy and civil liberties. In particular, we are concerned that the bill as written: (1) fails to ensure prior judicial review under a robust legal standard; (2) provides insufficient notice and transparency; (3) would attempt to require the compulsory production of user data from service providers pursuant to international agreements, counter to the CLOUD Act's intent; and (4) fails to provide a clear and robust mechanism for providers to challenge inappropriate and overbroad requests. Additionally, given the interaction between this proposed legislation and the expected CLOUD Act agreement between the United States and Australia, we urge the PJCIS to release the draft text of the agreement before the passage of the legislation, so that the interaction between the law and the agreement can be fully understood and assessed by relevant stakeholders.

Prior Judicial Review Under a Robust Standard

A critical safeguard for regimes that permit one country to seek communications data directly from providers in another country is that the requesting country must provide prior judicial review under a robust standard. Individualized review by an independent authority is a fundamental protection under international human rights law. Advocates, scholars and companies have noted that in order to preserve the rule of law and ensure confidence in government, it is essential that CLOUD Act bilateral agreements require prior independent judicial review of all non-emergency law enforcement demands for content. Prior approval by an independent, merit-based judicial authority is the only globally accepted structure that at least aims to protect fundamental rights. Although the CLOUD Act only requires "review or oversight by a court, judge, magistrate, or other independent authority" prior to or during the execution of the data request,[1] to protect human rights, CLOUD Act agreements should incorporate further safeguards, and prior merit-based judicial review is essential and should be the standard.

The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 does contain mechanisms for prior review, but it is unclear that these are sufficient to meet calls for independent and judicial review. The legislation allows for review of law enforcement demands by either a judge or a nominated Administrative Appeals Tribunal (AAT) member.[2] The Tribunal, however, is not a court; the AAT is part of the executive branch, falls under the portfolio of the Attorney General, and its members are appointed by the Governor-General.[3] Review by an executive branch official does not provide the independent authorization sought, and is not adequate to protect the rights of individuals.[4]

The standards that govern prior, independent judicial authorization should also be rigorous, providing adequate protection for personal privacy and against government overreach or abuse. Requests should only be approved when they are supported by specific evidence that demonstrates criminal conduct and that the data demanded is *needed* in connection with an investigation of a serious criminal offense. However, the *International Production Orders Bill* does not provide a robust standard, and instead sets forth a series of "matters" that judges or AAT members must consider for each type of International Production Order (IPO). These include "how much the information would be likely to assist in connection with the investigation by the enforcement agency of the offence/offences;"[5] "how much the privacy of any person or persons would be likely to be interfered with;" and "how much such methods would be likely to prejudice the investigation." There is no rule defining how authorities should weigh these

[1] Pub. L. 115-141
[2] *The Telecommunications Legislation Amendment (International Production Orders) Bill 2020,* pg.
[3] Administrative Appeals Tribunal Act 1975; https://www.aat.gov.au/about-the-aat
[4] This issue of independent oversight has come up as a part of the independent review being conducted by Dr. James Renwick of Telecommunications and Other Legislation Amendment (TOLA) Assistance and Access Act. His review of TOLA will be submitted in June 2020, with the inquiry by the Parliamentary Joint Committee on Intelligence and Security still on the necessity and proportionality of the Act ongoing.
[5] *The Telecommunications Legislation Amendment (International Production Orders) Bill 2020,* pg. 61

different factors or robust safeguards in place to ensure that the judge or AAT member meets certain standards when considering these factors. Rather, the bill appears to provide broad discretion to officials in conducting this review process.

A bilateral agreement under the U.S. CLOUD Act would permit the governments of Australia and the United States to make requests for communications data directly to providers in the other country. As companies and advocates alike have argued throughout the CLOUD Act debate, to ensure that this is a rights-protective regime, any government seeking to send law enforcement demands directly to a foreign provider must be required to implement prior independent judicial authorization based on a meaningful minimum legal and factual showing.[6] Judicial authorization under a robust privacy standard would provide a critical safeguard against overbroad and unlawful demands for customer data.

Notice and Transparency

Another key safeguard to protect human rights is the provision of meaningful notice to individuals. We are concerned, however, that the *International Production Orders Bill* does not include a mechanism requiring government officials to notify subjects of data requests, whether individuals or other entities, that access to their data has been requested. The three types of production orders identified in this bill, interception, stored communications, and telecommunications data all require the identification of a target whose information is being sought under the order.

In general, users have a universal right to notice. The *International Production Orders Bill* does not provide any requirement, or even mechanism, for government officials to notify data subjects of requests. We would note that unlike the U.K.'s Investigatory Powers Act, the *International Production Orders Bill* does not explicitly prohibit providers from providing notice to their customers. However, as the bill builds on the existing frameworks in place, it cannot be ignored that particularly the powers enshrined under TOLA prohibit notification and protect the data communications provider (DCP) from being sued directly by the individual if they are in breach of their rights. Providing notice -- even if delayed to where necessary to protect an ongoing investigation -- should be a duty of governments. It should not be left to the discretion of providers and individuals cannot be barred from exercising their rights. By including a requirement for notice Australia would ensure that best practices surrounding notice are maintained.

[6] https://na-production.s3.amazonaws.com/documents/Coalition_Letter_on_Cross_Border_.pdf; https://blogs.microsoft.com/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf

Under criminal law in the United States, giving proper notice through sufficiently particular warrants has always been the government's legal duty when it searches an individual's property, as it is crucial to having the ability to defend oneself. Though the U.S. Supreme Court has never considered directly whether stored electronic communications are entitled to Fourth Amendment protection, justices have recognized that lower court rulings holding that the Fourth Amendment requires law enforcement to obtain a warrant in order to access the contents of e-mails are appropriate, as e-mail should be given the same protections as traditional mail.[7] Advocates and companies alike have recognized the importance of providing notice to individual defendants (not simply to providers) regarding collection of their private communications.[8] Even in the intelligence context, where far fewer protections are generally offered to the subjects of surveillance, the U.S. government must provide notice to criminal defendants when it relies on communications data that has been gathered under Section 702 of the Foreign Intelligence Surveillance Act.

In addition, bilateral agreements under the CLOUD Act should provide for notice to the government of the provider's home country. We recognize that the goal of CLOUD bilateral agreements is to improve upon the onerous and prohibitively slow Mutual Legal Assistance Treaty process, so that government agencies in the provider's home country will no longer receive contemporaneous notice of international production orders. However, it is still important that the government of the provider's home country at least receive periodic consolidated notice of requests. This will enable each government to assess compliance with the bilateral agreement and to determine whether it should be renewed upon expiration. Moreover, considering the role that government agencies should play in at least tracking or monitoring requests, periodic notice to the provider's home country is important for purposes of transparency and accountability.

Compulsory Nature of IPOs

The CLOUD Act lifts the blocking provision under the Stored Communications Act (SCA) and authorizes U.S. service providers to disclose data to foreign governments pursuant to an executive agreement.[9] The CLOUD Act, however, does not serve as a basis for extra-territorial jurisdiction over foreign providers that Australia is asserting through the bill. Other provisions in the CLOUD Act reinforce the principle that the CLOUD Act merely lifted the blocking provision under the SCA and does not create extra-territorial jurisdiction that otherwise does not exist.

---

[7] *Carpenter v. United States*, 585 U.S. ___ (2018) slip op. at 21 (citing *United States v. Warshak, 631 F. 3d 266, 283–288 (CA6 2010)* with approval); *Carpenter v. United States*, 585 U.S. ___ (2018) slip op. at 13 (Kennedy, J., dissenting); *Carpenter v. United States*, 585 U.S. ___ (2018) slip op. at 15 (Gorsuch, J., dissenting).
[8] *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016); American Civil Liberties Union, "Why We're Supporting Microsoft's Challenge to Secret Surveillance," May 26, 2016. https://www.aclu.org/blog/privacy-technology/internet-privacy/why-were-supporting-microsofts-challenge-secret
[9] 18 USC 2702(b)(9); 18 USC 2702(c)(7).

The International Production Orders bill, however, is intended to apply extraterritorially, and would attempt to require the production of user data from service providers pursuant to international agreements, including executive agreements under the CLOUD Act.[10] The bill treats the mere existence of a CLOUD Act agreement as the basis for jurisdiction. Under the bill, the very fact that a provider is located in a country with whom Australia has an international agreement means that the provider is subject and ostensibly bound by an international production order. The bill thus exploits the CLOUD Act's removal of the SCA's blocking provision to create extraterritorial jurisdiction that would not otherwise exist (and does not exist for similarly situated providers located in other countries). The bill would seek to subject service providers to civil penalties if they fail to comply.[11] These provisions contravene the text and the spirit of the CLOUD Act.

Opportunity to Challenge

Internet users have an expectation that providers will have an opportunity to challenge unlawful demands in court prior to disclosure of their sensitive data. This expectation, and providers' ability to fulfill it, relies upon providers receiving sufficiently detailed legal process from governments that will allow them to identify and challenge overbroad and inappropriate demands. It also requires establishment of a clear procedure through which companies can bring such challenges. This ability to challenge demands provides users a critical check on governments' investigative powers, and is another procedure essential to the rule of law. Unclear legal processes, on the other hand, hamper this ability and useful check, endangering user rights.

The Internet Jurisdiction & Policy Network (I & J), an organization comprised of diverse stakeholders from civil society, academia, corporations, and governments, some of whom are also signers of this document, put forth useful criteria in assessing CLOUD agreements on this front. I & J recommends that any system providing cross-border access to communications data should: (1) "establish a procedure that protects the rights of providers to seek clarification from requesting countries about data requests/orders"; and (2) "establish a clear procedure for an independent authority to hear and adjudicate providers' challenges to data requests/orders." The I & J recommendations also outline the minimum procedural and substantive rights providers should have and more specific grounds upon which providers should be able to challenge data requests.[12]

The *International Production Orders Bill* fails to provide a sufficient procedure for challenges, and clear standards for approval or denial of those challenges. The bill does state, in Section 121,

[10] *The Telecommunications Legislation Amendment (International Production Orders) Bill 2020,* pg. 140.
[11] *Id*. at pg. 142-43.
[12] Pg. 21, Internet and Jurisdiction Policy Network's Data & Jurisdiction Program Report: Operational Approaches https://www.internetjurisdiction net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf

that providers "may, by written notice given to the Australian Designated Authority, object to the order on the grounds that the order does not comply with the designated international agreement," but only provides very vague procedures beyond that. Section 121 merely states that these objections must be "given to the Australian Designated Authority within a reasonable time" after receipt, and explain their reasoning. Additionally, although the bill allows for cancellations of orders in Section 122, and lays out procedures for the Australian Designated Authority to follow when cancelling orders, it provides no clear criteria or legal standards for decision-makers to follow in assessing whether an order should be cancelled.

An opportunity to challenge is only meaningful if providers are given clear procedural and substantive rights to challenge demands that are overbroad, abusive, violate the terms of an international agreement, or are otherwise unlawful. Providers must receive detailed legal processes from law enforcement to allow for a proper review of the relevant demand, and must also have clear mechanisms that have been laid out to them to challenge unlawful and inappropriate demands for user data to protect human rights. The *International Production Orders Bill* as written unfortunately does not meet this standard, and should be amended to include clear procedures and standards for provider challenges.

Conclusion

The undersigned organizations, companies, and individual experts appreciate the opportunity to submit these coalition comments in connection with the Committee's review.

Civil Society Organizations

Access Now

Blueprint for Free Speech

Center for Democracy & Technology

Constitutional Alliance

Defending Rights & Dissent

Electronic Frontier Foundation

International Civil Liberties Monitoring Group

Internet Society

New America's Open Technology Institute

Privacy International

Prostasia Foundation

Reporters Without Borders (RSF)

Restore The Fourth, Inc.

S.T.O.P. - The Surveillance Technology Oversight Project

TechFreedom

X-Lab

Technology Companies and Trade Associations

ACT | The App Association

Google

Reform Government Surveillance

Technical and Policy Experts*

Adam Shostack, Author, Threat Modeling: Designing for Security

Amie Stepanovich, Silicon Flatirons at Colorado Law

Corch, Managing Director, Shogun Cybersecurity

Dr. Christopher Parsons, Senior Research Associate, Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto

G.J. Turner (Perth, Australia)

Jeffrey J. Blatt, U.S. Technology Lawyer/U.S. Law Enforcement Officer

Mailyn Fidler, Research Affiliate, Berkman Klein Center for Internet & Society

Martin Silva Valent, Director, DATAS

Peter Swire, Professor, Georgia Institute of Technology

Riana Pfefferkorn, Associate Director of Surveillance and Cybersecurity, Stanford Center for Internet and Society

Dr. Richard Forno, Senior Lecturer, UMBC, Assistant Director, UMBC Center for Cybersecurity

Sascha Meinrath

Dr. Suelette Dreyfus

* Affiliations are provided solely for identification purposes