April 29, 2020

Issues of Concern under the CLOUD Act for Australian Legislation Amendment (International Production Orders) Bill 2020

These comments respond to the request for comment regarding the Australian Legislation Amendment (International Production Orders) Bill 2020 (the "Bill").[1] The focus of these comments is on the relationship between the Bill and the CLOUD Act, enacted in the United States in 2018.[2] An important goal of the Bill is to provide the legal structure required to draft and enact an executive agreement with the U.S. consistent with the CLOUD Act. Such an executive agreement would notably enable Australia to issue orders to investigate serious crimes directly to Designated Communications Providers ("DCPs") to access the content of communications by use of an International Production Order ("IPO"). In the absence of an executive agreement, DCPs that are U.S. service providers (including many of the largest global service providers) are subject to criminal and civil penalties if they provide the content of communications to a non-U.S. government such as Australia.

These comments perform a "gap analysis" of the Bill and the CLOUD Act, in order to identify areas where the Bill as currently drafted may not meet CLOUD Act requirements. Failure to meet such requirements could render Australia ineligible for an executive agreement under the CLOUD Act, even if the Bill is enacted.

The comments address seven topics: (1) judicial role; (2) lack of DCP ability to notify, especially to the U.S. Department of Justice ("US DOJ"); (3) scope limited to serious crime, not national security or terrorism generally; (4) institutional oversight requirements; (5) periodic review of implementation of the executive agreement; (6) limits on direct or indirect targeting of U.S. persons; and (7) encryption.

I. Judicial Role

The CLOUD Act states that an order "shall 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."[3]

As written, the Bill may violate this requirement. Specifically, concerning *prior* judicial review, the Bill enables orders by the Administrative Appeals Tribunal ("Tribunal").[4] It appears

[1] The Bill and official discussion of it are at: https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6511_first-reps/toc_pdf/20025b01.pdf;fileType=application%2Fpdf; https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6511_ems_0ac5ae09-3e3e-400b-ae5e-680a68af4e45/upload_pdf/733176.pdf;fileType=application%2Fpdf.

[2] For an explanation of the CLOUD Act, see Peter Swire & Jennifer Daskal, "Frequently Asked Questions about the CLOUD Act," Cross-Border Data Forum (Apr. 19, 2019), at https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act.

[3] 18 U.S.C. 2523(b)(4)(D)(v).

[4] *See* The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (stating in relevant part that in the context of an IPO for criminal law purposes, the relevant decision-maker which decides whether to issue an IPO under the Bill is: (i) For IPOS relating to interception, an "eligible Judge or nominated AAT member" (Clause 30 of the Schedule), or (ii) For IPOs relating to stored communications, an "issuing authority"

that the Tribunal, however, is neither a court nor an independent authority. Rather, my understanding is that the Tribunal is part of the executive branch under the portfolio of the Attorney General, and its members are therefore appointed by the Governor-General.[5] Consequently, the Tribunal may not constitute a "judge, magistrate, or other independent authority" as required by the CLOUD Act.

Relatedly, and as discussed in Section II below, the Bill quite possibly fails to provide sufficient "review or oversight" *after the fact*, for "proceedings regarding enforcement of the order." In particular, there is an absence of effective notice and enforcement mechanisms for DCP's receiving orders.

To address this apparent gap between CLOUD Act requirements and the Bill, the Bill might be amended to ensure sufficient oversight by judicial or other independent authorities. In the alternative, the executive agreement might state that only judicial orders, rather than orders by the AAT, would qualify under the executive agreement.[6]

II. Lack of DCP Ability to Notify, Including to US DOJ and Third Countries

There are three categories of concerns about the lack of notice provisions in the bill, concerning notice to US DOJ, those subject to the IPO, and third countries where there may be a conflict of law.

(a) US DOJ. The CLOUD Act provides that "the United States Government shall reserve the right to render the agreement inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked."[7]

The Bill, however, does not provide any provision for the DCP to give notice to outside parties. Without the ability of the DCP to give notice to the U.S. Department of Justice, there exists no mechanism for the U.S. government to enforce its right to block an improper order to a DCP. This lack of notice to US DOJ would appear to violate the CLOUD Act requirement cited above.

(b) Notice to subjects of an IPO. More broadly, the Bill is silent on the lawfulness of the DCP's ability to provide notice to those who are subjects of an IPO. The recipient of notice might be a company, such as when the IPO seeks email from a non-DCP company, where the email is also available to the DCP. The recipient of notice might also be an individual whose communications are subject to an IPO. Such notice is a central feature of the U.S. law of the Fourth Amendment (concerning government searches), although in some instances notice is allowed to be delayed until secrecy is no longer required to carry out the investigation of the crime. Although the CLOUD Act does not in so many words require such notice, it would be consistent

(Clause 39 of the Schedule). An 'issuing authority' is an authority appointed by the Attorney-General and may be either a judge of a court created by Parliament; a magistrate; or a Deputy President, senior member or member of the AAT (Clause 16 of the Schedule)).

[5] Administrative Appeals Tribunal Act 1975; https://www.aat.gov.au/about-the-aat.

[6] There has been a similar proposal previously, in connection with a possible CLOUD Act executive agreement between the U.S. and India. Under Indian law, an order for communications content can be made either by a judge or a police official. A previous publication has suggested that only judicial orders might qualify under a CLOUD Act agreement. DeBrae Kennedy-Mayo, Peter Swire, Sreenidhi Srinivasan & Madhulika Srikumar, "Indian-US Data Sharing for Law Enforcement: Blueprints for Reform," Observer Research Foundation/Georgia Tech Cross-Border Requests for Data Project (Jan. 17, 2019), https://www.orfonline.org/research/india-us-data-sharing-for-law-enforcement-blueprint-for-reforms-47425.

[7] 18 U.S.C. 2523(b)(4)(K).

with the principles and practice of U.S., and with the protection of fundamental rights, for such notice to be permitted for the IPO.

(c) Notice to third countries. One important goal of the CLOUD Act was to speed legitimate criminal investigations by reducing conflict-of-law problems. An executive agreement under the CLOUD Act is designed to speed such investigations, by reducing conflicts between existing U.S. law and the law of a country such as Australia seeking evidence from a DCP.

Conflicts of law issues can readily arise, however, concerning the laws of third countries. As one example, the European Union's General Data Protection Regulation may create conflicts when a country (such as Australia) seeks evidence held by U.S. service provider concerning data processed in the E.U.[8] In order to achieve the CLOUD Act goal of speeding legitimate criminal investigations and reducing conflicts of law, there should be a provision legally enabling notice to third country governments, such as those in the E.U. The executive agreement between the U.S. and United Kingdom enables such notice to third countries.[9]

(d) Conclusion. The Bill as drafted appears to lack provisions for adequate notice, to ensure that US DOJ (and others) could be notified.

III. Scope Limited to Serious Crime, Not National Security or Terrorism Generally

The CLOUD Act provides that "an order issued by the foreign government—''(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;"[10]

The Bill does define a "serious offence," essentially for crimes with a maximum penalty of at least 3 years, or 7 years for an interception order. A difficulty arises, however, because the Bill authorizes three distinct types of orders: (i) orders for "enforcement of the criminal law;" (b) "control orders," which concern anti-terrorism activities; and (iii) orders relating to national security. The latter two categories create possible violations of the CLOUD Act requirements – it is not clear whether an order under those two categories would be consistent with the CLOUD Act. A DCP, in order to ascertain the lawfulness of an IPO (and in order to comply with U.S. criminal and civil laws), must know whether the request is for prosecution of a "serious crime."

Clear labelling of the legal basis for an IPO would appear to be necessary for a DCP to determine whether the order is lawful. Such labelling would need to identify a serious crime, even for criminal law orders. For control orders and national security orders, there would be additional concern that the IPO does not in fact meet the CLOUD Act requirement that an order be for a serious crime.

From the current text of the Bill, it is not clear, at least to this non-Australian lawyer, that the required specific notice concerning a serious crime is authorized or required by the Bill.

---

[8] *See* Theodore Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities after the CLOUD Act: Is There a Conflict with the GDPR?", (June 14, 2019), https://ssrn.com/abstract=3397047; Peter Swire, "When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis of Transfer," (Oct. 19, 2019), SSRN: https://ssrn.com/abstract=3473187.

[9] Article 5(10) of that agreement states: "In cases where an Order subject to this Agreement is issued for data in respect of an individual who is reasonably believed to be located outside the territory of the Issuing Party and is not a national of the Issuing Party, the Issuing Party's Designated Authority shall notify the appropriate authorities in the third country where the person is located, except in cases where the Issuing Party considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights.'

[10] 18 U.S.C. 2523(b)(4)(D)(i).

Relatedly, if the Bill does not change on this point, then US DOJ would have an obligation to ensure procedures are in place to determine whether each DCP is for a serious crime. It is a matter of Australian law whether the legal structures for such notice are in place.

IV. Institutional Oversight Requirements

The CLOUD Act contains multiple provisions requiring effective management and oversight of requests, to ensure compliance with the CLOUD Act requirements. These institutional provisions include provisions requiring that the foreign government:

> "(iv) Has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities."
> (v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government."[11]

Similarly, the CLOUD Act requires that:

> "(F) the foreign government shall promptly review material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures; [and]
> (G) the foreign government shall, using procedures that, to the maximum extent possible, meet the definition of minimization procedures."[12]

However, currently, the Bill is unclear as to the extent to which Australian institutional structures currently exist or are authorized by current law to serve these purposes. To the extent there is no legal structure to implement all of the above, the Bill would be insufficient to enable a CLOUD Act executive agreement.

V. Periodic Review of Implementation of the Executive Agreement

The CLOUD Act provides that "the foreign government shall agree to periodic review of compliance by the foreign government with the terms of the agreement to be conducted by the United States Government."[13] It further requires that "The Attorney General, with the concurrence of the Secretary of State, shall review and may renew a determination [that the Executive Agreement meets the requirements of the CLOUD Act] every 5 years."[14]

The CLOUD Act thus requires institutions and reporting to be in place sufficient to enable review of operation of the executive agreement within a period not to exceed five years. As mentioned in II, above, the current Bill may not have sufficient notice requirements to enable case-by-case review by US DOJ of the lawfulness of an IPO. The additional point to consider is whether

[11] 18 U.S.C. 2523(b)(1)(B).
[12] 18 U.S.C. 2523(b)(4).
[13] 18 U.S.C. 2523(b)(4)(J).
[14] 18 U.S.C. 2523(e)(1).

case-by-case notice and overall transparency are sufficient to enable the periodic review. In order to successfully negotiate an executive agreement with US DOJ, there must be enough transparency about operations of the IPO's to enable the required review. Assuming such transparency and legal structure is authorized under the Bill, a subsequent executive agreement may further specify the ways that such review might operate.

VI. Limits on Direct or Indirect Targeting of US Persons

In addition to these general institutional requirements, the CLOUD Act includes specific provisions limiting the targeting of U.S. persons and dissemination of information concerning U.S. persons. Specifically, the CLOUD Act provides that:

> "(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement; [and]
> (B) the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States."[15]

The CLOUD Act also includes institutional protections including that:

> "(2) the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;"[16] and
> "(H) the foreign government may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud."

These prohibitions on direct or indirect targeting and the institutional requirements in respect of United States persons are not explicitly provided for in the Bill. An important legal question is whether the necessary institutional arrangements would have a lawful basis once the Bill passes. For instance, would there be authorization and funding available in specific Australian agencies to install these targeting, dissemination, and other requirements? To reach an executive agreement, US DOJ would need to determine that the requisite institutional arrangements can and would exist. In addition, US DOJ would need a way to review the actual operations of such activities, in order to meet the requirements for periodic renewal of the executive agreement.

VII. Encryption

The CLOUD Act provides that ''(3) the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from

[15] 18 U.S.C. 2523(b)(4)(A-B).
[16] 18 U.S.C. 2523(b)(2).

decrypting data."[17] A similar encryption provision exists in the U.S. Communications Assistance to Law Enforcement Act of 1994, which states: "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[18]

There appears to be a potentially important conflict between the CLOUD Act encryption provision and Australian law if the Bill is enacted. In short, the Bill (and subsequent executive agreement) would appear to have the effect of creating an "obligation that providers be capable of decrypting data."

As background, the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the "Assistance and Access Bill"), includes provisions that create mechanisms for both voluntary and mandatory assistance to law enforcement's and intelligence agencies' decryption activities.[19] Specifically, the Assistance and Access Bill creates a framework of voluntary Technical Assistance Requests and mandatory Technical Assistance Notices and Technical Capability Notices. As part of this framework, government entities may request Designated Communication Providers remove "one or more forms of electronic protection that are or were applied by, or on behalf of, the provider."[20]

Under current law, it is illegal for a U.S. service provider to supply the content of communications in response to a non-U.S. government request. Instead, a government such as Australia uses the Mutual Legal Assistance Treaty process, with an MLAT request going to US DOJ. Under U.S. law there is no mandatory technical assistance such as Australian law states. Therefore, with an MLAT request, there would currently be no legal mechanism in the U.S. to impose "an obligation that providers be capable of decrypting data."

If the Bill becomes law, and an executive agreement exists, then the Australian government would be able to seek the content of communications directly from a CPD under an IPO. The Australian government would also have available the Assistance and Access Bill. Together, the Australian government could then claim it can require mandatory technical assistance from a CPD.

That ability to claim such assistance would be *due to* the executive agreement. The result would appear to be creating an "obligation that providers be capable of decrypting data." Thus, it would appear that a CLOUD Act executive agreement is at least in serious tension with the encryption provision of the CLOUD Act.

This apparent violation of the CLOUD Act appears to be an important issue worthy of informed discussion and analysis. A solution could be to amend the Bill to ensure that this result does not occur. Alternatively, the executive agreement itself could block such a possibility. Given the longstanding concern in the U.S. Congress about maintaining strong encryption in telecommunications, for security and other reasons, failure to address this encryption issue may become an important point of criticism in U.S. review of any executive agreement.

Conclusion

[17] 18 U.S.C. 2523(b)(4)(H).

[18] 47 U.S.C. 1002(b)(3).

[19] *See generally*, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Australian Parliament, https://www.legislation.gov.au/Details/C2018A00148.

[20] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Australian Parliament, Section 317E(1)(a).

In conclusion, thank you for the opportunity to offer comments on your important initiative to prepare for the possibility of an executive agreement between Australia and the United States. To make that executive agreement a reality, the Bill and other Australian law must enable the executive agreement to meet the requirements of the CLOUD Act. These comments are intended to assist the process, by identifying possible problems and suggesting some ways to address such problems.