COVINGTON

CLOUD Act Creates New Framework for Cross-Border Data Access

March 27, 2018

Data Privacy and Cybersecurity

On March 23, 2018, Congress passed, and President Trump signed into law, the Clarifying Lawful Overseas Use of Data ("CLOUD") Act, which creates a new framework for government access to data held by technology companies worldwide.

The CLOUD Act, enacted as part of the Consolidated Appropriations Act, has two components.

Part I: Extraterritorial Reach of U.S. Orders and Comity Rights for Providers

The first part of the CLOUD Act provides that orders issued pursuant to the Electronic Communications Privacy Act ("ECPA") can reach data regardless of where that data is stored. This portion of the law addresses the question at the heart of *United States v. Microsoft*, the Supreme Court case that was argued on February 27.*

Part I of the Act also creates a new statutory mechanism by which technology companies can challenge warrants based on the material risk of a conflict with the laws of qualified foreign countries—specifically, those countries that enter into bilateral agreements of the type contemplated in Part II of the Act and that afford reciprocal comity rights to the United States (referred to as a "qualifying foreign governments"). The CLOUD Act also preserves the common law rights of providers to bring comity challenges based on conflicts of laws with *other* countries (*i.e.*, those that are *not* "qualifying foreign governments" under the Act).

Under this new statutory comity framework, a provider may file a motion to modify or quash U.S. legal process if it reasonably believes: (1) the customer or subscriber is not a U.S. person and does not reside in the United States, and (2) the required disclosure would create a material risk of violating the laws of a qualifying foreign government.

In any such challenge, a court may modify or quash the legal process upon finding that: (1) the required disclosure would violate the qualifying foreign government's law, and (2) the interests of justice dictate that the legal process should be modified or quashed. In conducting this second inquiry, courts are to consider a series of comity factors set out in the statute. During the pendency of such a challenge, the provider may notify the qualifying foreign government of the existence of the legal process and thereby allow the foreign government to raise any concerns directly with the U.S. Government.

Part II: Framework for Bilateral Agreements on Cross-Border Data Requests

The second part of the CLOUD Act creates a framework for new bilateral agreements with foreign governments for cross-border data requests. Under these bilateral agreements, the

United States and participating foreign governments would remove legal restrictions that otherwise prohibit technology providers from complying with the other country's legal requests.

Previously, governments had to invoke mutual legal assistance treaties ("MLATs") to obtain evidence stored in another country. Under the MLAT process, a foreign government seeking information from a U.S. provider would ask the U.S. Department of Justice to obtain a U.S. court order for that information. Part II of the CLOUD Act creates a new framework that instead allows foreign governments to serve legal process directly on U.S. providers, without the necessity of first making an MLAT request to the U.S. Department of Justice.

Because the CLOUD Act has no effect on a foreign government's jurisdiction over U.S. companies, any obligation by a provider to comply with a foreign order issued pursuant to such an agreement must arise under the foreign law. In other words, the CLOUD Act removes barriers that might otherwise prohibit a U.S. provider from complying with a foreign government's order, but the CLOUD Act does not compel a U.S. provider to comply with any foreign order.

Not all governments can enter into bilateral agreements under the CLOUD Act. Before a country may do so, the Attorney General must submit certain written certifications to Congress regarding the foreign country. Those certifications must find that the country meets specific criteria establishing that its domestic law affords robust substantive and procedural protections for privacy and civil liberties. Additionally, the foreign government must adopt procedures to minimize the acquisition and retention of information about U.S. persons and cannot impose a decryption obligation on providers through the agreement.

Bilateral agreements must also contain a number of limits on the types of orders that may be submitted by the foreign government directly to a U.S. provider, including:

- Orders must be for the purpose of obtaining information relating to a serious crime, including terrorism.
- Orders must identify a specific person, account, address, device, or other identifier.
- Orders must comply with the foreign government's domestic law.
- Orders must be based on requirements for a reasonable justification based on articulable and credible facts.
- Orders must be subject to judicial review prior to, or in enforcement proceedings regarding, enforcement of the order.
- Orders for interceptions must be for a fixed and limited time, may not last longer than reasonably necessary to accomplish the order's purposes, and may only be issued if the same information could not be obtained by a less obtrusive method.
- Orders may not be used to infringe freedom of speech.

Foreign governments that enter such bilateral agreements must also agree to periodic compliance reviews by the U.S. Government.

Finally, the CLOUD Act contains specific provisions addressing how these bilateral agreements will be entered into and renewed. Under those provisions, once the Attorney General certifies a new agreement, it is to be considered by Congress. The agreement will enter into force unless Congress enacts a joint resolution of disapproval within 180 days. Every five years, the Attorney

General is to review his or her determination that a foreign country meets the requirements for entering into a bilateral agreement. If he renews that determination, he is to submit a report to Congress containing the reasons for the renewal, any substantive changes to the agreement or to foreign law, and how the agreement has been implemented and what problems or controversies, if any, have arisen.

[*] *Covington represents Microsoft Corporation in* United States v. Microsoft*, No. 17-2.*

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

James Garland	+1 202 662 5337	jgarland@cov.com
Alex Berengaut	+1 202 662 5367	aberengaut@cov.com
Lisa Peets	+44 20 7067 2031	lpeets@cov.com
Marty Hansen	+44 20 7067 2239	mhansen@cov.com
Kate Goodloe	+1 202 662 5505	kgoodloe@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.