JONES DAY

COMMENTARY

MARCH 2018

Congress Passes CLOUD Act to Facilitate Law Enforcement Access to Overseas Data

IN SHORT

The Situation: The U.S. Congress passed the CLOUD Act amending U.S. surveillance laws to facilitate law enforcement access to the contents of communications and other related data.

The Result: U.S. law enforcement authorities can compel production of communications data even if it is stored outside the United States, and certain foreign countries may be eligible to enter into executive agreements with the United States that would permit U.S. service providers to respond to certain foreign orders seeking access to communications data.

Looking Ahead: Providers of electronic communications and certain cloud services should be prepared to respond to legal process under the new regime, while both providers and users of their services should consider the implications for their businesses.

As part of the omnibus budget legislation signed into law on March 23, 2018, the U.S. Congress enacted the Clarifying Overseas Use of Data ("CLOUD") Act. The Act addresses two festering issues concerning cross-border law enforcement access to communications data: (i) it resolves the question presented in the pending Supreme Court case, *United States v. Microsoft*, by generally permitting U.S. law enforcement to obtain communications content and related data even if it is stored overseas; and (ii) it permits U.S. service providers to respond to foreign legal process seeking access to stored communications data or intercepts that do not target U.S. persons or those located in the United States, but only if the country has entered into an executive agreement with the United States that meets certain criteria.

U.S. Law Enforcement Access to Data Stored Overseas

Prior to the CLOUD Act, the law did not specify whether the U.S. government could compel disclosure of content of communications that a service provider had stored abroad. In *Microsoft*, the parties agreed that the relevant statute did not permit extraterritorial application of a warrant seeking communications content. Microsoft argued that the warrant would be applied extraterritorially because the search would occur on its overseas server; the government argued that it would not because disclosure of information would occur in the United States.

> Prior to the CLOUD Act, the law did not specify whether the U.S. government could compel disclosure of content of communications that a service provider had chosen to store abroad.

The CLOUD Act resolves this issue—and likely renders the *Microsoft* case moot—by specifying that a service provider served with a warrant or other appropriate legal process must turn over contents or other information within its "possession, custody, or control," regardless of where that information is stored. A provider can move to quash if it reasonably believes that: (i) the subscriber is a non-U.S. person who resides outside the United States; and (ii) complying with the process would create a material risk that the provider would violate the laws of a "qualifying foreign government"—that is, a government that has entered into an executive agreement to facilitate cross-border law enforcement access to data (see below). In such cases, a court is to conduct a comity analysis to help determine whether the provider should be required to comply. The Act does not provide guidance as to whether a provider may move to quash in other circumstances, although it includes a savings clause providing that current common law comity standards continue to apply.

Foreign Law Enforcement Requests to U.S. Providers

Prior to the CLOUD Act, the law prohibited U.S. providers from complying with foreign legal process seeking stored communications contents or intercepts. The CLOUD Act now permits providers to comply with such foreign legal process, but only if the request: (i) does not target U.S. persons or persons located in the United States; and (ii) comes from a country that has struck an executive agreement with the United States. The Act specifies requirements for such executive agreements that attempt to ensure that the country has robust legal protections for privacy and civil liberties and that orders issued under the agreement relate only to serious crimes and meet requirements akin (but not necessarily identical) to those in U.S. law, including oversight by a court or other independent authority. The United States and United Kingdom negotiated an agreement in anticipation of this change in law, but it remains to be seen what other countries enter into similar agreements.

TWO KEY TAKEAWAYS

1. Providers of electronic communications and certain cloud services should analyze how the Act will apply to them and be prepared to respond to legal process under the new regime.
2. Companies and individuals who use such services should consider whether the privacy and other implications of the Act require any change in their practices.

CONTACTS


Samir C. Jain
Washington

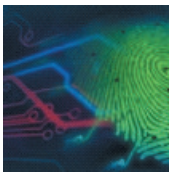

James T. Kitchen
Pittsburgh


Undine von Diemar
Munich


Jörg Hladjk
Brussels

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>

SEC Releases Guidance on Public Company Cybersecurity Disclosures



Appellate Court Limits Who May Sue Under Biometric Information Privacy Act

China's New Cybersecurity Law Brings Enforcement Crackdown

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.