wiley

NEWSLETTER

CLOUD Act Passes in Omnibus Spending Bill, Impacting User Data Stored Overseas

April 2018

Privacy in Focus®

On March 23, 2018, President Trump signed a $1.3 trillion spending package that will keep the government funded through the end of September. The Omnibus bill includes the Clarifying Lawful Overseas Use of Data Act (CLOUD Act or Act), a bill proposed in February that will allow U.S. law enforcement to access citizens' data stored overseas and clarify the legality of similar requests coming from foreign law enforcement agencies for data on their citizens stored in the United States.

The Act may have significant implications for companies that receive requests from U.S. or foreign law enforcement for user data. While issues about data localization will continue – indeed, it may be impossible for a single government to resolve those issues – the Act takes steps to clarify the ability of U.S. law enforcement and certain foreign governments to obtain user data across borders.

Domestic Law Enforcement Requests for User Data Stored Overseas

The CLOUD Act amends the Stored Communications Act (SCA), a 1986 law enacted long before the advent of cloud computing and the construction of storage centers around the world. The CLOUD Act makes clear that U.S. law enforcement can reach user data stored overseas, adding the following section to the SCA:

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to *preserve, backup, or disclose the contents of a wire or electronic*

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

communication and any record or other information pertaining to a customer or subscriber within such provider's *possession, custody, or control,* regardless of whether such communication, record, or other information is located within or outside of the United States." (Emphasis added.)

The Act also gives providers the right to apply for a motion to quash or modify legal process if the provider reasonably believes the subscriber is not a U.S. person and that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government. It also requires a court to conduct a comity analysis in the event of a motion to quash.

Modified Procedures for Handling Foreign Law Enforcement Requests

Congress recognized that communications-service providers sometimes face conflicting legal obligations when a foreign government orders production of electronic data that United States law may prohibit providers from disclosing. To address these conflicts, the CLOUD Act creates a mechanism whereby Congress, working with the U.S. Departments of Justice and State, can enter into an "Executive Agreement" with approved foreign governments. Under the Act, communications service providers are permitted to respond to certain requests from foreign governments that are covered by an Executive Agreement.

Executive Agreements will only be approved "if the Attorney General, with the concurrence of the Secretary of State," determines that:

1. The country has "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" (to be determined by reference to a comprehensive list of human rights and rule of law standards);
2. The foreign government has adopted minimization procedures regarding information concerning U.S. persons; and
3. The agreement has protections to prevent the foreign government from targeting or collecting information about U.S. persons or persons located in the U.S., and to prevent the U.S. government from requesting the foreign government to use the agreement as a runaround on current restrictions on data collection.

Orders issued under the agreements must relate only to serious crimes and meet a number of other requirements. For example, Orders must provide a "reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"; be "subject to review or oversight by a court, judge, magistrate or other independent authority"; and cannot be used "to infringe freedom of speech," among other limitations.

United States v. Microsoft Corp.

The Act clarifies issues that have led to years of litigation, most notably the recent dispute between U.S. law enforcement and Microsoft. In October 2017, the Supreme Court of the United States granted certiorari in *United States v. Microsoft Corp.* to address whether an email service provider must comply with a warrant

supported by probable cause under the SCA when the email records are stored outside of the United States. The SCA authorizes the government to obtain email records when it has a warrant supported by probable cause to believe a crime is being committed.

In *Microsoft*, a federal judge issued a warrant, which was served on Microsoft at its headquarters in Redmond, Washington. The warrant required Microsoft to disclose information about an email account that the government believed was being used for drug trafficking. Microsoft refused to comply, arguing that the SCA did not apply because the emails were stored in Ireland. The trial court disagreed with Microsoft, but the U.S. Court of Appeals for the Second Circuit reversed and refused to enforce the warrant because of what it found to be an extraterritorial effect. The Supreme Court heard argument in February, and the case is now pending.

Passage of the CLOUD Act is likely to moot the case, and Microsoft supports the Act. The Court took up the case to determine whether the SCA was intended to cover data controlled by U.S. companies but held overseas. The CLOUD Act amends the SCA to require production of user data overseas, likely resolving that question.