Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Law Enforcement Access to Overseas Data Under the CLOUD Act

Stephen P. Mulligan
Legislative Attorney

May 2, 2018

Law enforcement officials in the United States and abroad frequently seek access to electronic communications, such as emails and social media posts, stored on servers and in data centers in foreign countries. Because the architecture of the internet allows technology companies to store data at a great distance from the physical location of their customers, electronic communications that could serve as evidence of a crime often are not housed in the same country where the crime occurred. This disconnect has caused both the United States and foreign governments to seek access to data stored outside their territorial jurisdictions. In the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Congress enacted one of the first significant changes in decades to U.S. law governing cross-border access by law enforcement to electronic communications held by private companies.

U.S. Law Enforcement's Ability to Obtain Data Overseas

Passed as part of the Consolidated Appropriations Act of 2018, the CLOUD Act has two major components. The first facet addresses the U.S. government's ability to compel technology companies to disclose the contents of electronic communications stored on the companies' servers and data centers overseas. The Stored Communications Act (SCA)—which was enacted as Title II of the broader Electronic Communications Privacy Act of 1986 (ECPA)—mandates that certain technology companies disclose the contents of electronic communications pursuant to warrants issued by U.S. courts based on probable cause that the communications contain evidence of a crime. But a dispute arose over whether warrants issued under the SCA could compel U.S. companies to disclose contents of communications stored outside the United States when Microsoft refused to disclose the contents of an MSN.com email that was located in a datacenter in Ireland. While the Supreme Court was set to resolve this issue in *United States v. Microsoft*, the CLOUD Act amended the SCA to require that technology companies provide data in their possession, custody, or control in response to an SCA warrant—regardless of whether the data is located in the United States. On April 17, 2018, the Supreme Court ruled that the

Congressional Research Service
7-5700
www.crs.gov
LSB10125

change in law mooted the *Microsoft* case.

The first facet of the CLOUD Act also addresses potential conflicts of law that could arise if the United States seeks data stored in a foreign country and the law of that country prohibits the data's disclosure. The CLOUD Act seeks to resolve these potential conflicts between U.S. and foreign law in a manner informed by principles of comity—or respect for foreign sovereignty. Among other things, principles of comity have been understood to permit courts to excuse violations of U.S. law, or moderate the sanctions imposed for such violations, when the violations are compelled by a foreign nation's law. When an extraterritorial data demand under the SCA could result in a violation of the law of certain select countries with which the United States has a data sharing agreement (discussed below), the CLOUD Act creates a statutorily defined comity analysis to address the potential conflict. This statute-based comity analysis requires a U.S. court to consider several enumerated factors when considering whether to quash or modify a warrant seeking data stored in a country that has a data sharing agreement with the United States. For those nations with no data sharing agreement, the CLOUD Act's statutorily guided comity analysis does not apply, but the CLOUD Act states it preserves the more general, common law principles of comity.

A New Form of International Data Sharing Agreement

The second facet of the CLOUD Act addresses the reciprocal issue of foreign governments' ability to access data in the United States as part of their investigation and prosecution of crimes. Prior to the CLOUD Act, foreign nations seeking data in the United States were required to request the assistance of the U.S. government through either mutual legal assistance treaties (MLATs) or judicial instruments known as letters rogatory. Requests under either instrument are reviewed by U.S. courts before disclosure to the foreign nation can be authorized, but U.S. and foreign officials have criticized the processes as inefficient and unable to accommodate the increasing number of transnational data requests by law enforcement in the digital era.

The CLOUD Act responds to calls for modernization by authorizing the executive branch to conclude international agreements through which select foreign governments can seek data directly from U.S. technology companies without individualized review by the U.S. government. Agreements authorized by the CLOUD Act would remove the legal restrictions on certain foreign nations' ability to seek data directly from U.S. providers in cases involving "serious crimes," provided that the data requests do not target U.S. persons, and so long as the Executive has determined that the foreign nation's laws adequately protect privacy and civil liberties, among other requirements (discussed in this CRS Report).

Before an agreement made pursuant to the CLOUD Act can enter into force, the Attorney General, with the concurrence of the Secretary of State, must make four written certifications to Congress:

1. the foreign nation's domestic law "affords robust substantive and procedural protections for privacy and civil liberties" in its data-collection activities, as determined based on at least seven statutory factors;
2. the foreign government has adopted "appropriate" procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons;
3. the executive agreement will not create an obligation that providers be capable of decrypting data, nor will it create a limitation that prevents providers from decryption; and
4. the executive agreement will require that any order issued under its terms will be subject to an additional set of procedural and substantive requirements (analyzed here).

Commentary on the CLOUD Act

The CLOUD Act's authorization of a new form of cross-border data sharing agreement has garnered both praise and criticism from observers. Some argue that the Act provides a practical remedy for problems

related to the globalization of evidence and the increased demand for data stored overseas in criminal cases. Supporters assert that law enforcement's need for data stored abroad, which often is held by U.S. internet companies, has overburdened the legal architecture established in the MLAT and letters rogatory systems, rendering those systems outdated and inefficient. Several major U.S. technology companies—including Apple, Facebook, Google, Microsoft, and Oath—support the legislation and believe that it will reduce potential conflict of laws.

Critics of the CLOUD Act argue that it poses a threat to civil liberties and human rights by lowering the standards previously necessary to obtain evidence in cross-border criminal investigations and prosecutions. They contend, among other things, that the executive branch's decision to certify a country as satisfying the CLOUD Act's standards should be subject to judicial or other review. Other critics believe that the certification process is problematic because foreign governments' real-world operations may not comport with their domestic laws and may change over time.

What is Congress's Role under the CLOUD Act?

Commentary on the CLOUD Act may be of interest to Congress because the Act expressly provides for a mandatory 180-day period of congressional review before a proposed data sharing agreement can enter into force. The Act also defines a number of procedures authorizing congressional consideration of a joint resolution of disapproval of an executive agreement on an expedited process (discussed here). Congress can block a proposed agreement from entering into force by enacting a joint resolution of disapproval during the 180-day window.