The Long Arm of Cyber Law: How the CLOUD Act Expands Government Access to Overseas Data

May 14, 2018

With cyber crimes on the rise—including international email scams and overseas investment frauds—Congress has erased many of the boundaries that have impeded government access to data stored in the United States and abroad. Enacted on March 23, the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act) ushers in a new legal framework for foreign and domestic law enforcement agencies seeking access to electronic data relevant to a criminal investigation. Given the trends identified in the FBI’s latest Internet Crime Report, any company transmitting or storing information about individuals or corporations, whether in the US or abroad, should become familiar with the CLOUD Act’s procedural requirements.

The CLOUD Act is intended to resolve two principal issues: (1) access by US law enforcement to data stored by US companies abroad, and (2) access by foreign law enforcement to data stored in the US. Both companies that transmit electronic communications and that store data remotely—ECS and RCS services, respectively—should not only understand the implications of these changes, but also develop procedures to file motions to modify or quash orders determined to be potentially unlawful.

When Can US Law Enforcement Access Data Stored by US Companies Abroad?

First, the CLOUD Act removes any doubts about the ability of US law enforcement to serve warrants or issue subpoenas under the Stored Communications Act (SCA) for data that US companies store abroad. Prior
to the CLOUD Act, this question was awaiting resolution before the Supreme Court in *Microsoft v. US*, which addressed whether a US company must comply with a warrant for data stored by the company outside the US. The CLOUD Act now clarifies that the SCA applies to any “communication, record, or other information . . . located within or outside of the United States.” (The Supreme Court dismissed the *Microsoft* case as moot based on the CLOUD Act’s enactment and the government’s subsequent procurement of a new warrant.) US companies must be aware that SCA warrants and subpoenas now require preservation, backup, or disclosure of information stored in the US and abroad. Foreign companies with a US subsidiary or other presence in the US should consider the possibility that US law enforcement may use the law to demand information stored overseas.

**When Can Foreign Law Enforcement Access Data Stored in the US?**

Second, the CLOUD Act offers a streamlined alternative to the “blocking” provision of the SCA, which acted to prevent ECS and RCS companies from complying with demands for information from foreign law enforcement issued directly to the company. Until now, foreign governments were required to enter into Mutual Legal Assistance Treaties (MLATs) with the US, under which the foreign government could submit requests for information from US companies through the Department of Justice, and US law enforcement could submit requests for information from foreign companies through a reciprocal agreement. MLATs have been much critiqued, blamed for creating backlogs at DOJ and limiting due process for the recipient US company.

Under the CLOUD Act, the Attorney General, with the concurrence of the Secretary of State, has a new option: entering into executive agreements with countries that comply with a set of requirements related to privacy protections, freedom of expression, international human rights obligations, and trial rights. Notably, the Act directs the Attorney General to consider whether a candidate country “has adequate substantive and procedural laws on cybercrime and electronic evidence demonstrated by being a party to the [Budapest] Convention on Cybercrime” or through similar domestic laws. The Budapest Convention requires signatories to criminalize certain types of computer crimes, implement harmonized procedures for preserving, searching, seizing, and intercepting data, and cooperate with other signatories on extradition and related procedures. The inclusion of the Budapest Convention and references to international human rights law, privacy protections, and prohibitions against arbitrary detention as criteria for executive agreements under the CLOUD Act implies that the US will likely enter into such agreements with longstanding allies such as the United Kingdom, Japan, and Australia. “Qualifying foreign governments” that enter into an executive agreement under the CLOUD Act may issue an order seeking content, records, and trap and trace/pen register information from a US company about a non-US person for purposes of detecting,
Under What Circumstances Can a Demand for Data Under the CLOUD Act Be Quashed?

A US company receiving an order under the CLOUD Act may move to quash the demand based on a reasonable belief that disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government when the subject of the request is not a US person and does not reside in the US. A motion to quash may be particularly relevant to foreign companies with US subsidiaries facing the same circumstances, which will ultimately require a US court to find whether a CLOUD Act order conflicts with relevant law in the parent company's home jurisdiction.

Notably, this statutory right to quash is “without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.” This provision raises some uncertainty over whether a provider may bring a motion to quash based on conflicts of law with other governments—for example, in the context of a US commissioner's subpoena based on a request from a non-qualifying country. Also left unresolved is whether a company could move to quash a demand from a qualifying country if the demand would violate the laws of a non-qualifying country where the provider is also regulated or subject to liability or whether a US court will permit a motion to quash from a foreign company in a non-qualifying country. It is unclear whether the savings clause was intended to reach these situations, and the issue will likely have to be resolved in future litigation.

ECS and RCS companies are therefore now faced with a new legal regime for foreign access to user or subscriber information: qualifying foreign governments may submit a demand directly to the US provider, subject only to a motion to modify or quash, while non-qualifying foreign governments must still participate in the time-consuming MLAT process. Providers should take the time to understand the various country-specific data protection and disclosure regimes to which they may be accountable and determine whether, and under what circumstances, a motion to quash based on a demand from a qualifying foreign government might be appropriate.

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Steve Bunnell, an O’Melveny partner licensed to practice law in the District of Columbia, Ronald Cheng, an O’Melveny partner licensed to practice law in California, Randall W. Edwards, an O’Melveny partner licensed to practice law in California, Scott Pink, an O’Melveny special counsel licensed to practice law in California, Eric Goldstein, an O’Melveny associate licensed to practice law in Maryland, and Antoinette Rangel, an O’Melveny associate licensed to practice law in New York,
The Long Arm of Cyber Law: How the CLOUD Act Expands Government Access to Overseas Data

May 14, ...

AUTOMATED VEHICLES: A ROADMAP

MOMENTUM NEWS CAREERS ALUMNI RESOURCES LANGUAGE