Congress Enacts Law Clarifying Reach of Warrants for Overseas Data

MARCH 26, 2018

On Friday, March 23, President Trump signed into law the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amends the Stored Communications Act (SCA), 18 U.S.C. § 2701, *et seq.*, to require providers of electronic communication services or remote computing services to produce data sought by the government under the SCA, regardless of whether the data are located within or outside the United States. The CLOUD Act creates a limited mechanism for providers to challenge legal requests for data held abroad and creates a framework for responding to requests for electronic communications from foreign governments.[1] The Act thus represents a legislative response to the question about the SCA's extraterritorial reach that is pending before the Supreme Court in *United States v. Microsoft Corp.*, No. 17-2 (argued Feb. 27, 2018). How the Court will respond to adoption of the Act remains to be seen.[2]

I. The SCA and Data Stored Abroad

Making clear what had previously been an open question under the SCA, the CLOUD Act expressly requires providers to comply with the SCA's data retention and disclosure obligations regardless of where the data are stored. It states that providers must "comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic 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." CLOUD Act § 103(a) (to be codified at 18 U.S.C. § 2713).

The CLOUD Act also provides a mechanism for certain service providers to challenge a warrant issued under the SCA in some cases. A provider of electronic communication service "to the public" or remote computing service may move to quash or modify the warrant if the provider reasonably believes: (1) that the customer or subscriber is not "a United States person" and does not reside in the United States; and (2) that the disclosure would "create a material risk that the provider would violate the laws of a "qualifying foreign government." CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)). A "qualifying foreign government" is one that has entered into an executive agreement with the United States with elements described further below and "the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under" the SCA as amended by the CLOUD

Act. CLOUD Act § 103(b).

The motion must be filed within fourteen days of service of the warrant. *Id.* Upon receiving the motion, the court must allow the governmental entity seeking the data to respond. *Id.* The court may then grant the motion if it determines that: (1) the disclosure would force the provider to violate the laws of a "qualifying foreign government"; (2) the customer or subscriber is not a U.S. person or resident; and (3) "based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed." *Id.*

In its "totality of the circumstances" analysis, the court must consider, "as appropriate": (1) the interests of the United States, including the requesting governmental entity; (2) the interests of the qualifying foreign government in preventing disclosure; (3) the likely penalties the provider and its employees may suffer "as a result of inconsistent legal requirements imposed on the provider"; (4) the location and nationality of the subscriber or customer whose communications are being sought, and the nature and extent of that person's connections to the requesting governmental entity; (5) the provider's ties to and presence in the United States; (6) the importance to the investigation of the information sought; (7) the likelihood of timely and effective access to the information through alternative means; and (8) in the case of a foreign request, the investigative interests of the foreign authority making the request. *Id.*

Importantly, the CLOUD Act does not provide a mechanism to challenge warrants or other legal process requesting data of targets who are United States persons or residents. Nor does it authorize providers to challenge warrants that would require them to violate the laws of a foreign country that is not a "qualifying foreign government." But it includes two provisions expressly preserving companies' ability to raise certain challenges. Section 103(b) adds to the SCA a new provision (codified at 18 U.S.C. § 2703(h)(5)(B)), which reserves the right to challenge gag orders. And Section 103(c) provides that the Act doesn't disrupt existing rights to challenge legal process on comity grounds in cases not involving qualifying foreign governments.

II. The SCA and Data Requests from Foreign Governments

The CLOUD Act also establishes a framework for "qualifying foreign governments" to request data stored in the United States. As noted above, a "qualifying foreign government" is one that has entered into an executive agreement with the United States with elements described further below and "the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under" the SCA as amended by the CLOUD Act. CLOUD Act § 103(b).

To satisfy the definition of "qualifying foreign government," a country must enter into an executive agreement with the United States that the Attorney General, with the concurrence of the Secretary of State, certifies in writing to Congress satisfies four sets of criteria. CLOUD Act § 105.

First, the Attorney General must determine that the foreign government's domestic law provides "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." *Id.* This determination must "take[] into account, as appropriate, credible information and expert input." *Id.* In

making this determination, the Attorney General must consider several factors, including whether the foreign government: (1) "has adequate substantive and procedural laws on cybercrime and electronic evidence"; (2) "demonstrates respect for the rule of law and principles of nondiscrimination"; (3) "adheres to applicable human rights obligations and commitments or demonstrates respect for international universal human rights"; (4) "has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement"; (5) "has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government"; and (6) "demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet." *Id.*

Second, the Attorney General must certify that the foreign government "has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement." *Id.*

Third, the Attorney General must determine that "the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data." *Id.*

Fourth, the Attorney General must determine that the executive agreement with the foreign government contains numerous safeguards, including, among others, that the foreign government may not target U.S. persons (or persons outside the United States if the purpose is to obtain information concerning a United States person or resident), that orders issued by the foreign government must be related to a serious crime and must be in compliance with that country's domestic law, and that the foreign government must take steps to preserve and secure the material collected. *Id.*

The Attorney General's determinations are not subject to judicial or administrative review, but they are subject to congressional review. *Id.* Within seven days of certifying an executive agreement, the Attorney General must submit the agreement and his or her determinations to the Senate and House Judiciary Committees, the Senate Committee on Foreign Relations, and the House Committee on Foreign Affairs. *Id.* The executive agreement becomes effective 180 days later, unless Congress enacts a joint resolution of disapproval pursuant to procedures established in the Act. *Id.*

Once an executive agreement meeting these criteria has taken effect, providers of electronic communication service to the public and providers of remote computing service may comply with orders issued by a foreign government that is a party to the executive agreement, and such disclosures are exempt from the prohibition against disclosure in § 2702. CLOUD Act § 104 (to be codified at 18 U.S.C. § 2511(2)).

III. Conclusion

The CLOUD Act clarifies provider obligations to produce foreign-stored data to U.S. law enforcement agencies, and it establishes a framework that may ultimately allow service providers to disclose

communications to certain foreign governments. The extent of providers' ability to object to requests for data held overseas and the extent of foreign government requests to which providers will be subject will turn on how many executive agreements meeting the extensive statutory requirements the United States enters into with foreign governments.

---

[1] The text of the CLOUD Act, H.R. 1625, 115th Cong., 2d Sess. div. V, §§ 101-106 (2018), may be found here.

[2] In a letter filed in the Supreme Court on Friday, March 23, the United States informed the Court that it is currently evaluating "whether, and if so, to what extent the passage of the CLOUD Act affects the Court's disposition" of the *Microsoft* case. The government's letter may be found here.