April 23, 2018

Supreme Court Dismisses *Microsoft* Appeal as Moot After Passage of the CLOUD Act

As reported in our earlier client memorandum,[1] in February 2018, the U.S. Supreme Court heard argument in *United States* v. *Microsoft Corp.*, a case concerning the government's ability to compel U.S. service providers to disclose email communications electronically stored outside the U.S. On April 17, 2018, the Court dismissed the appeal as moot based on the recent enactment of the CLOUD Act.

This memorandum describes the Court's holding and discusses the statutory framework of the CLOUD Act, which now governs disputes such as that in the *Microsoft* case.

The Supreme Court's Decision in *Microsoft*

The *Microsoft* case arose when the U.S. government obtained a warrant under Section 2703 of the Stored Communications Act (SCA) for email content and information from a Microsoft Network (msn.com) email account, and Microsoft moved to quash the warrant on the basis that the information requested was stored on servers outside the U.S., specifically in Ireland. The legal question presented was whether a probable-cause-based warrant issued by a Magistrate Judge under the SCA reaches digitally-stored materials within a provider's control but stored abroad. The Court of Appeals for the Second Circuit, reversing the District Court, held that the SCA did not require service providers to produce email content stored outside the U.S. The Supreme Court granted certiorari and heard argument on February 27, 2018.

Several weeks later, on March 23, 2018, Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which directly addressed the question implicated in the *Microsoft* case concerning the extraterritorial reach of the SCA. In particular, the CLOUD Act amends the SCA, expressly requiring email service providers to preserve, back up, and disclose to law enforcement electronic data within their "possession, custody, or control," even when that data is located outside the U.S. The Department of Justice subsequently obtained a new warrant for the email account at issue in the *Microsoft* case under Section 2703 of the now-amended SCA. In light of these events, the Court found that there was no longer a "live dispute" between the U.S. and Microsoft. The Court therefore vacated the judgment below, remanding the case to the Second Circuit with instructions to direct the District Court to dismiss the case as moot.

---

[1] Available at www.paulweiss.com/media/3977647/28feb18microsoft.pdf.

The Governing Framework Under the CLOUD Act

The CLOUD Act reflects Congress's effort to clarify the ability of law enforcement to obtain email communications stored abroad. Although the CLOUD Act provides that an email service provider can be compelled under the SCA to produce electronic data stored outside the U.S., it also imposes certain limitations and permits service providers to challenge warrants or other legal process issued under the SCA in certain circumstances. For example, under the CLOUD Act, a service provider may seek to modify or quash a warrant or other legal process issued under the SCA on the basis of a conflict of laws with a "qualifying foreign government," which is defined as a government with which the U.S. has entered into an executive agreement under the CLOUD Act. To successfully challenge a warrant, a service provider must demonstrate that: (1) the customer or subscriber is not a U.S. person and does not reside in the U.S.; and (2) the required disclosure would create a material risk that the provider would violate the laws of the qualifying foreign government.[2] While such a motion is pending, service providers must preserve, but are not obligated to produce, the information sought.[3] A court may grant such a motion only if it finds that both of the above-referenced requirements are met and that, based on the totality of the circumstances, the "interests of justice" require that the legal process should be modified or quashed.[4]

If the above circumstances do not exist, the CLOUD Act's savings clause provides another mechanism for a service provider potentially to seek to quash or modify a warrant or other legal process issued under the SCA. That clause provides that law enforcement actions under Section 2703 of the SCA are to be evaluated by "the common law standards governing the availability or application of comity analysis."[5] These standards are not specifically defined, and the CLOUD Act does not provide any specific guidance on how and when this comity analysis limits the reach of the SCA to information stored outside the U.S.

The CLOUD Act's Impact on the Reach of Foreign Governments

In addition to expressly authorizing the U.S. government to compel the production of electronic information stored abroad, the CLOUD Act also modifies the process for foreign governments seeking access to data stored in the U.S.

Previously, foreign governments could only access data stored in the U.S. by making diplomatic requests for the data to the U.S. The process was governed by mutual legal assistance treaties, or MLATs, which must be ratified by a supermajority vote in the Senate. The CLOUD Act, however, allows the President to make executive agreements that will govern foreign access. The Act states that the Attorney General must

---

2 *See* CLOUD Act, Section 103(b), to be codified at 18 U.S.C. § 2703(h)(2).

3 *See* CLOUD Act, Section 103(b), to be codified at 18 U.S.C. § 2703(h)(4).

4 *See* CLOUD Act, Section 103(b), to be codified at 18 U.S.C. § 2703(h)(2)-(3).

5 CLOUD Act, Section 103(c).

submit a written certification to Congress that the agreement complies with the requirements of the Act, a determination that is not subject to judicial or administrative review. Such executive agreements will be effective 180 days after notice is provided to Congress, unless Congress enacts a joint resolution of disapproval.[6]

The Attorney General must certify that a number of requirements have been met, including: that the foreign country's domestic law affords "robust" protections for privacy and civil liberties; that it has adequate laws regarding cybercrime and electronic evidence; that it demonstrates respect for the rules of law; that it adheres to applicable human rights obligations; and that it has clear legal mandates and procedures governing the collection, use, and oversight of data.[7]

A foreign government's request for information must relate to the prevention, detection, investigation, or prosecution of a serious crime. The Act provides that the foreign government's procedures must follow the domestic law of that country and does not provide for the application of U.S. due process protections.

The Act does provide for periodic review of compliance by the U.S. and states that the U.S. government may render the agreement inapplicable in specific cases if it concludes that it does not apply to a particular request.

The Act also limits the ability of foreign governments to obtain information concerning individuals residing in the U.S. The Attorney General must certify that the foreign government has "adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons." Additionally, a foreign government may not intentionally target a U.S. person or a person located in the U.S.; it also may not target a non-U.S. person located outside the U.S. if the purpose is to obtain information concerning a U.S. person or a person located in the U.S.[8]

The passage of the CLOUD Act represents a significant change in the ways in which cross-border data access is governed. It remains unclear how the procedures and limitations established in the Act will work in practice.

* * *

6 *See* CLOUD Act Section 105, to be codified at 18 U.S.C. § 2523(a)-(d).

7 *See* CLOUD Act Section 105, to be codified at 18 U.S.C. § 2523(b)(1)(A)-(B).

8 *See* CLOUD Act Section 105, to be codified at 28 U.S.C. § 2523(b)(2)-(4).

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Lorin L. Reisner
+1-212-373-3250
lreisner@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Associate Rebecca L. Orel contributed to this Client Memorandum.