SULLIVAN & CROMWELL LLP

April 19, 2018

U.S. Supreme Court Dismisses *U.S.* v. *Microsoft* as Moot After CLOUD Act Signed Into Law

Court Declares That There is No Longer a Live Controversy Over a Warrant Requiring Microsoft to Disclose Customer Data Stored Overseas.

SUMMARY

On October 16, 2017, the U.S. Supreme Court granted a petition for *certiorari* in *United States* v. *Microsoft Corp.*, No. 17-2, to resolve whether the U.S. Department of Justice ("DOJ") may use the Stored Communications Act ("SCA") to issue warrants compelling companies subject to U.S. jurisdiction to disclose customer data stored abroad. The Court held oral argument on the case on February 27, 2018.[1]

On March 23, 2018, President Trump signed the Clarifying Lawful Overseas Use of Data ("CLOUD") Act, which created a new legislative scheme for law enforcement to access data stored overseas. DOJ promptly issued a new warrant to Microsoft under the CLOUD Act. As a result, both Microsoft and DOJ filed submissions with the Supreme Court stating that the old subpoena was moot and the case no longer presented a live controversy. On April 17, 2018, the Supreme Court agreed, vacated the petition for *certiorari* and the judgment below, and remanded with instructions to dismiss the case as moot.

In addition to mooting the *Microsoft* case, the CLOUD Act has major implications for how electronic communications are disclosed in federal criminal investigations. The Act presumes that DOJ may subpoena electronic communications, records, and other information within the possession, custody, or control of companies subject to the jurisdiction of the United States. The Act also sets forth a framework through which the United States can enter into agreements with other countries to facilitate the mutual

production of information stored in those countries or the United States, and the factors that must be considered if a company moves to quash any such subpoena.

BACKGROUND

Enacted in 1986, the SCA authorized the government to secure statutory warrants to obtain electronic communications data stored by electronic service providers (such as e-mails hosted by Google's Gmail and Microsoft's MSN). In relevant part, Section 2703(a) of the SCA provides that:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication . . . only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure [requiring a finding of probable cause] (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. . . .[2]

The dispute between Microsoft and DOJ arose in December 2013, when DOJ secured a probable cause-based warrant under Section 2703 to compel Microsoft to disclose data from an email account. Microsoft moved to quash the warrant. Microsoft stated that it stored the data in Ireland, and argued that DOJ's authority under the SCA extended only to data located in the United States and that DOJ could not compel the company to retrieve data stored in Ireland and disclose it to U.S. law enforcement authorities. According to Microsoft, DOJ was required to make its data request to Irish authorities pursuant to the two countries' Mutual Legal Assistance Treaty ("MLAT"). DOJ countered by arguing that the SCA authorizes law enforcement to require companies subject to the jurisdiction of the United States to turn over data within their custody and control that is responsive to an SCA warrant regardless of where that data is stored, and that Microsoft could easily retrieve the relevant data through one of its U.S. facilities. As such, DOJ argued that it was not required to proceed under the MLAT process

Then-Chief Judge Loretta A. Preska of the U.S. District Court for the Southern District of New York denied Microsoft's motion to quash and required the company to comply with the warrant.[3] On appeal, the U.S. Court of Appeals for the Second Circuit reversed Judge Preska's decision,[4] holding that SCA warrants cannot compel the production of data stored overseas, because statutes are "'meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears."[5] As such, the panel concluded that using an SCA warrant to force Microsoft to "interact with the Dublin datacenter to retrieve . . . [its customer's] data [that] lies within the jurisdiction of a foreign sovereign" and produce that data to U.S. authorities was an impermissible extraterritorial application of the statute.[6]

In a concurring opinion, Judge Lynch wrote "to emphasize the need for congressional action to revise a badly outdated statute," which could not have anticipated recent technological advances, including the advent of cloud storage for data, when the SCA was enacted in 1986.[7] The DOJ petitioned the Supreme Court for a writ of *certiorari*, which the Court granted on October 16, 2017.

Less than one month after *Microsoft* was argued at the Supreme Court, President Trump signed the CLOUD Act into law. The Act enjoyed broad support from DOJ, Microsoft, and the broader tech community.[8] Critical to situations like the one presented in *Microsoft*, the CLOUD Act added the following four provisions.

First, to clarify the territorial reach of a Section 2703(a) warrant, the CLOUD Act added a new Section 2713 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 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*.[9]

This language unambiguously manifests Congress' intent that warrants issued under the SCA require production of data in situations identical to *Microsoft* where data is stored abroad.

Second, the CLOUD Act creates the opportunity for a new system of executive agreements between the United States and "qualifying foreign governments" that will help companies navigate the difficulties of facing inconsistent legal obligations in different jurisdictions compelling them simultaneously to produce and withhold data.[10] To become part of this new system as a qualifying foreign government, countries may enter into an agreement with the United States only after agreeing to grant reciprocal rights to data access to the United States, being certified by the Attorney General and Secretary of State as "afford[ing] robust substantive and procedural protections for privacy and civil liberties" concerning data collection, and guaranteeing that they will provide certain protections for the data of U.S. persons.[11] Moreover, because these executive agreements will work bilaterally, they will ensure that there is a system that addresses qualified foreign government requests for data stored in the United States.[12]

Third, if the United States has an executive agreement in place with a qualifying foreign government, CLOUD Act Section 103[13] also provides that a company required to disclose its customer's data under its possession, custody, or control has a statutory right to move to quash an SCA warrant if it reasonably believes that the customer is neither a "United States person"[14] nor a resident of the United States and that the required disclosure would create a material risk of violating the laws of a qualifying foreign government. In turn, a court may grant the motion if:

> (1) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
>
> (2) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
>
> (3) the customer or subscriber is not a United States person and does not reside in the United States.[15]

To determine "the interests of justice," in point 2 above, the court is to consider:

> (1) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
>
> (2) the interests of the foreign qualifying government in preventing any prohibited disclosure;
>
> (3) the likelihood, extent, and nature of penalties to the provider or any employee of the provider as a result of inconsistent legal requirements imposed on the provider;
>
> (4) [t]he nature and extent of the subscriber or customer's connection to the United States . . .[16];
>
> (5) the nature and extent of the provider's ties to and presence in the United States;
>
> (6) the importance to the investigation of the information to be disclosed;
>
> (7) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
>
> (8) if the legal process has been sought on behalf of a [foreign qualifying government], the investigative interests of the foreign authority making the request for assistance.[17]

Finally, the CLOUD Act clarifies that, when the statutory comity analysis is not applicable to the case, such as when the data is being stored in a country that is not a qualified foreign government with an executive arrangement with the United States, the company moving to quash or modify the SCA warrant may still argue that common-law principles of comity dictate that the warrant be quashed or modified.[18]

Shortly after the CLOUD Act's passage, on March 30, 2018, DOJ obtained a new SCA warrant to replace the original warrant contested by Microsoft.[19] The Government argued that this new warrant mooted the case because it was issued under the CLOUD Act and so "Microsoft no longer has any basis for suggesting that such a warrant is impermissibly extraterritorial because it reaches foreign-stored data, which was the sole contention in [Microsoft's] motion to quash."[20] Microsoft did not oppose the Government's motion and the Supreme Court declared the case moot, vacated the decision of the Second Circuit, and remanded with instructions to dismiss the case in a *per curiam* opinion.[21]

IMPLICATIONS

First, with respect to the *Microsoft* case, the Supreme Court's ruling did not end the matter entirely. Microsoft indicated that it will evaluate the new warrant, which leaves the door open for the company to challenge the scope of the warrant on comity grounds if it determines that a conflict with Irish law might arise from disclosing its customer's data to U.S. authorities. Unless Ireland enters into an executive agreement with the United States and becomes a qualified foreign government, which has not been reported as imminent, Microsoft's comity argument would only be on common-law grounds as opposed to the statutory comity analysis detailed in the CLOUD Act.

Second, once this system of executive agreements with qualified foreign governments is in place it will provide greater certainty for large communications companies, like Microsoft, that operate on a global scale and for smaller companies that store user data across international boundaries. From a law

enforcement perspective, the CLOUD Act helps avoid the undesirable situation where criminals evade law enforcement by storing their electronic data in multiple jurisdictions.

Third, executive agreements will create a framework for qualified foreign governments to access data stored in the United States.

* * *

ENDNOTES

[1] *See United States Supreme Court Grants Certiorari in United States* v. *Microsoft Corporation*, SULLIVAN & CROMWELL LLP (Oct. 17, 2017), https://www.sullcrom.com/united-states-supreme-court-grants-certiorari-in-united-states-v-microsoft-corporation.

[2] 18 U.S.C. § 2703(a) (2012).

[3] Judge Preska summarily affirmed Magistrate Judge James C. Francis IV's decision from *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

[4] *See In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 209, 220–22 (2d Cir. 2016).

[5] *Id.* at 210 (quoting *Morrison* v. *Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)).

[6] *Id.* at 220-21.

[7] *Id.* at 222–33 (Lynch, J., concurring).

[8] *See* Press Release, Sen. Orrin Hatch, The CLOUD Act: It's Time for Our Laws to Catch Up with Our Technology (Feb. 26, 2018), https://www.hatch.senate.gov/public/index.cfm/2018/2/the-cloud-act-it-s-time-for-our-laws-to-catch-up-with-our-technology; Brad Smith, *The CLOUD Act Is an Important Step Forward, But Now More Steps Need to Follow*, MICROSOFT: BLOG (Apr. 3, 2018), https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

[9] CLOUD Act § 103(a)(1), 18 U.S.C. § 2713 (2018) (emphasis added).

[10] The CLOUD Act defines a "qualifying foreign government" as one that has an executive agreement with the United States under the new CLOUD Act Section 105 (described below) and has laws that grant service providers similar substantive and procedural protections to those provided by the United States. CLOUD Act § 103(b), 18 U.S.C. § 2703(h)(1)(A) (2018).

CLOUD Act Section 105, in turn, provides for a system of executive agreements on access to data by foreign governments. For a foreign country to be eligible to enter into an agreement with the United States, it must grant reciprocity for data access rights to the United States, and also the Attorney General and Secretary of State must determine that the foreign country's laws provide "robust substantive and procedural protections for privacy and civil liberties" with respect to data protection. *Id.* § 105(a), 18 U.S.C. § 2523(b)(1), (4)(I). Further, the CLOUD Act protects U.S. citizens' data by providing that foreign countries must comply with requirements such as ensuring there are procedures in place to minimize the acquisition, retention, and dissemination of U.S. persons' data, not intentionally targeting U.S. persons' data without going through proper diplomatic channels with DOJ first, and not targeting foreigners located abroad to obtain U.S. persons' data. *Id.*, 18 U.S.C. § 2523(b)(4)(A)–(C), (F)–(H). Finally, any disclosure order from the foreign country must meet certain minimum requirements akin to U.S. warrants such as being particularized and limited in scope, being approved by a judge (or other independent authority), being legal, and not infringing on free speech. *Id.*, 18 U.S.C. § 2523(b)(4)(D)–(E).

[11] CLOUD Act § 105(a), 18 U.S.C. § 2523(b)(1) (2018); *see also supra* note 10 (listing requirements for a country to be considered "qualifying").

[12] *See* CLOUD Act § 105(a), 18 U.S.C. § 2523(b)(4) (2018).

[13] CLOUD Act § 103(b), 18 U.S.C. § 2703(h)(2) (2018).

[14] The CLOUD Act defines a "United States person" as "a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States." CLOUD Act § 105(a), 18 U.S.C. § 2523(a)(2) (2018).

ENDNOTES (CONTINUED)

15 CLOUD Act § 103(b), 18 U.S.C. § 2703(h)(2)(B) (2018).

16 If the legal process has been sought on behalf of a foreign country, then courts must analyze the nature and extent of the customer's connection with that foreign country. CLOUD Act § 103(b), 18 U.S.C. § 2703(h)(3)(D) (2018).

17 CLOUD Act § 103(b), 18 U.S.C. § 2703(h)(3) (2018).

18 CLOUD Act Section 103(c) states the law's rule of construction, which provides that nothing in the CLOUD Act "shall be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis to other types of compulsory process or to instances of compulsory process issued under section 2703 (*i.e.*, SCA warrants) and not covered by the comity analysis under Section 2703(h)(2). CLOUD Act § 103(c), 18 U.S.C. § 2703 note (2018).

19 Motion to Vacate Judgment & Remand with Directions to Dismiss as Moot at 9, *United States* v. *Microsoft Corp*., No. 17-2 (U.S. Mar. 30, 2018).

20 *Id.*

21 *United States* v. *Microsoft Corp.*, No. 17-2, 2018 WL 1800369 (U.S. Apr. 17, 2018) (per curiam).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York

Nicolas Bourtin	+1-212-558-3920	bourtinn@sullcrom.com
Justin J. DeCamp	+1-212-558-1688	decampj@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Robert J. Giuffra Jr.	+1-212-558-3121	giuffrar@sullcrom.com
Camille L. Orme	+1-212-558-3373	ormec@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com