SULLIVAN & CROMWELL LLP

October 17, 2017

United States Supreme Court Grants *Certiorari* in *United States* v. *Microsoft Corporation*

Court Will Review Whether a Warrant Issued Under the U.S. Stored Communications Act Compels a U.S.-Based Entity to Disclose User Account Data Stored Abroad

SUMMARY

On October 16, 2017, the United States Supreme Court granted the petition for *certiorari* in *United States* v. *Microsoft Corp.*, No. 17-2. That case presents the question whether a U.S.-based entity (Microsoft) must comply with a probable cause-based warrant issued under Section 2703 of the Stored Communications Act ("SCA") and disclose to the United States Department of Justice ("DOJ") certain customer data stored abroad. The Supreme Court will review the decision issued last year by the United States Court of Appeals for the Second Circuit that Microsoft did not have to comply with an SCA warrant seeking certain customer data stored in its Dublin, Ireland datacenter, notwithstanding that the data was under Microsoft's control and could be retrieved from the United States.

The Supreme Court's decision may have significant implications for the ability of law enforcement agencies to obtain communications data stored outside the United States, and also for companies that must navigate among the competing demands of U.S. law enforcement requests, customer privacy expectations, and foreign laws. In addition, the Supreme Court's decision to review this issue comes as Congress considers legislation to expand the scope of U.S. warrants to cover data stored outside the United States.

BACKGROUND

In December 2013, DOJ secured an SCA warrant based on probable cause (of narcotics trafficking) that compelled Microsoft to disclose data from a web-based email account belonging to one of its customers. Microsoft complied with the warrant to the extent that the customer's data was located within the United States, but refused to disclose relevant data stored in Microsoft's Dublin, Ireland datacenter[1] and moved to quash the warrant to the extent that it sought such data. In its motion, Microsoft argued that the SCA warrant could not compel a U.S. entity to produce data stored overseas, and that DOJ could instead seek to obtain the data through the mutual legal assistance treaty governing the procedure for U.S. authorities to gather evidence in Ireland. A Magistrate Judge denied Microsoft's motion to quash on the basis that the SCA warrant operated like a traditional search warrant in that it requires a judge to find probable cause, but like a grand jury subpoena in that it seeks business records of a domestic entity stored abroad under the entity's control.[2] Then-Chief Judge Preska of the United States District Court for the Southern District of New York summarily affirmed the Magistrate Judge's decision. Microsoft was subsequently held in civil contempt for its failure to disclose the customer data and appealed the ruling to the Second Circuit.

On appeal, Microsoft argued that the SCA warrant was more akin to a traditional warrant, which cannot compel the seizure of materials outside the United States. The Second Circuit panel adopted Microsoft's argument in reversing the District Court's decision, holding that an SCA warrant could not compel the production of customer data stored abroad.[3] The Second Circuit panel concluded that the SCA does not apply extraterritorially because it cannot overcome the presumption that statutes are "'meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears."[4] Here, the court found that the purpose and language of the SCA supported the conclusion that the SCA only compels disclosure of data stored within the United States and that there was no express or implied contrary intent by Congress that the SCA apply extraterritorially. The court noted that in using the term "warrant," Congress incorporated not only the heightened scrutiny standard applied to traditional warrants, which may only be issued upon a finding of probable cause by a neutral magistrate, but also the territorial limitations of a traditional warrant.

In reaching this conclusion, the court also found that Congress's purpose in enacting the SCA was to provide basic safeguards for domestic users and protect the privacy of those users' stored communications. According to the panel, communications covered by the SCA—which are private to the customer—enjoy more robust protections than business records of a company that contain a customer's information, in which the customer has a diminished expectation of privacy. To support its conclusion, the panel observed that the Second Circuit has "never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item."[5]

Finally, the panel concluded that compelling a service provider to access and produce customer information stored abroad would be an illegal extraterritorial application of the SCA.[6] Thus, the crux of the Second Circuit's holding is that the location where the stored data is *stored*, as opposed to the location(s) from which the data can be electronically *retrieved*, is dispositive on the issue of extraterritoriality. Therefore, the panel held that federal prosecutors could not compel Microsoft to "interact with the Dublin datacenter to retrieve . . . [its customer's] data [that] lies within the jurisdiction of a foreign sovereign," even though Microsoft could have retrieved that data electronically from within the United States.[7]

In a concurring opinion, Judge Lynch stated that he did not believe this case to implicate individual privacy concerns, because the Fourth Amendment requirement for obtaining a warrant from a magistrate based on probable cause was met.[8] 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 it was enacted in 1986.[9]

After the Second Circuit's decision, DOJ sought a rehearing *en banc*, which was denied by an evenly divided Second Circuit.[10] The judges who dissented from the denial of the rehearing *en banc* noted that, although the SCA does not have an extraterritorial reach, "[e]xtraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant."[11] As Judge Jacobs noted, "no extraterritorial reach is needed to require delivery in the United States of the information sought, which is easily accessible in the United States at a computer terminal."[12] Here, "[t]he warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought. It need only touch some keys in Redmond, Washington."[13] According to Judge Raggi's dissent, "the only territorial event that needs to be warranted under the SCA is disclosure [and, thus n]o warrant was needed for Microsoft lawfully to access material on its Dublin servers from the United States."[14] Similarly, Judge Cabranes' dissent cautioned that the decision would restrict an "essential investigative tool" and has thus "burdened the government's legitimate law enforcement efforts," while "creat[ing] a roadmap for the facilitation of criminal activity."[15]

The government then petitioned the Supreme Court for a writ of *certiorari*, which was granted on October 16, 2017.

IMPLICATIONS

There are a number of important implications and considerations for both law enforcement entities as well as companies that store customer information abroad.

First, were the Supreme Court to reverse the Second Circuit, and adopt the logic of the dissenting and lower court opinions, it would expand the circumstances in which U.S.-based companies may find themselves caught between a U.S. law enforcement request or court order, and laws of foreign jurisdictions that may prohibit the act sought by that request or order. Here, U.S.-based companies compelled by an SCA warrant to produce communications stored abroad could face competing requirements from foreign jurisdictions that may prevent companies them from allowing certain customer information to leave the jurisdiction without customer consent.

Second, the case will be heard by the Supreme Court against the backdrop of significant Congressional debate on the topic which began following the proceedings in this case. As Microsoft points out in its argument opposing the government's petition for *certiorari*, "Congress is actively considering amendments to the SCA that would expressly provide for limited extraterritorial reach."[16] For example, the proposed International Communications Privacy Act, which was introduced in July 2017, would clarify the scope of when U.S. law enforcement agencies can obtain foreign-stored electronic communications. Under the proposed legislation, Microsoft would have been required to comply with the warrant.[17]

*   *   *

ENDNOTES

[1] Microsoft maintains that its customers' data is stored based on proximity to the physical home location self-identified by the customer to reduce network latency.

[2] *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).

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

[4] *Id.* at 210 (quoting *Morrison* v. *National Australia Bank Ltd.*, 561 U.S. 247, 255 (2010)).

[5] *Id.* at 215; *but see Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 855 F.3d 53, 72–73 (2d Cir. 2017) (Raggi, J., dissenting) (questioning this language and noting that the Second Circuit has "upheld the use of a subpoena to compel a caretaker to produce client materials in its domestic possession") (hereinafter, "*Warrant en banc* Denial").

[6] *Matter of Warrant*, 829 F.3d at 220.

[7] *Id.*

[8] *Id.* at 222–25 (Lynch, J., concurring).

[9] *Id.* at 232–33 (Lynch, J., concurring).

[10] *Warrant en banc* Denial, 855 F.3d 53.

[11] *Id.* at 61 (Jacobs, J., dissenting).

[12] *Id.* at 61.

[13] *Id.* at 61 (Jacobs, J., dissenting); *see id.* at 72 (Raggi, J. dissenting) ("Microsoft did not need any warrant from the United States to take possession of the subscriber communications it had stored in Ireland. Nor did it need such a warrant to transfer those communications from Ireland to the United States. Indeed, it did not need the approval of Irish authorities or even of its subscriber to take such action.").

[14] *Id.* at 72 (Raggi, J., dissenting).

[15] *Id.* at 63 (Cabranes, J., dissenting) (internal quotations and citations omitted).

[16] Microsoft, Opp. to *Cert*. at 14.

[17] International Communications Privacy Act, S. 1671, 115th Cong. § 3(a)(2)(A) (proposing to amend SCA § 2703 to read:

> "A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is stored, held, or maintained by the provider, *regardless of where such contents may be in electronic storage or otherwise stored, held, or maintained*, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.'')

(emphasis added).

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

Garrard R. Beeney	+1-212-558-3737	beeneyg@sullcrom.com
Nicolas Bourtin	+1-212-558-3920	bourtinn@sullcrom.com
David H. Braff	+1-212-558-4705	braffd@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Justin J. DeCamp	+1-212-558-1688	decampj@sullcrom.com
Christopher J. Dunne	+1-212-558-4115	dunnec@sullcrom.com
Stephen Ehrenberg	+1-212-558-3269	ehrenbergs@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Robert J. Giuffra, Jr.	+1-212-558-3121	giuffrar@sullcrom.com
Suhana S. Han	+1-212-558-4647	hans@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Sharon L. Nelles	+1-212-558-4976	nelless@sullcrom.com
Matthew J. Porpora	+1-212-558-4028	porporam@sullcrom.com
Yvonne S. Quinn	+1-212-558-3736	quinny@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Jeffrey T. Scott	+1-212-558-3082	scottj@sullcrom.com
Samuel W. Seymour	+1-212-558-3156	seymours@sullcrom.com
Karen Patton Seymour	+1-212-558-3196	seymourk@sullcrom.com
Marc Trevino	+1-212-558-4239	trevinom@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com

Palo Alto			
	Laura Kabler Oswell	+1-650-461-5679	oswelll@sullcrom.com
London			
	Juan Rodriguez	+44-20-7959-8499	rodriguezja@sullcrom.com
Other			
	Michael Rosenthal	+32-7870-5001	rosenthalm@sullcrom.com