February 28, 2018

U.S. Supreme Court Hears Oral Argument on Extraterritorial Reach of Email Search Warrants in *Microsoft* Case

As reported in our earlier Client Alert (https://www.paulweiss.com/media/3977440/19oct17-microsoft.pdf), the U.S. Supreme Court granted certiorari in *United States* v. *Microsoft Corp.*, U.S. No. 17-2, a high-profile case that could have a major impact on how and where corporations store the electronic information of their customers. On February 27, 2018, the U.S. Supreme Court heard oral argument in the case.

The case arises from a narcotics investigation in which the U.S. government sought a warrant to obtain email content and information from a Microsoft Network (msn.com) email account. Magistrate Judge James C. Francis IV of the Southern District of New York issued the warrant under Section 2703 of the Stored Communications Act (SCA). Microsoft moved to quash the warrant to the extent it sought customer information stored on servers in Ireland, arguing that U.S. courts do not have the authority to issue SCA warrants for data stored overseas. Judge Francis denied Microsoft's motion. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014). Then-Chief Judge Loretta Preska of the Southern District of New York adopted Judge Francis's conclusions and affirmed his ruling. On appeal, the Second Circuit reversed and remanded with instructions to quash the warrant, holding that the SCA does not apply extraterritorially and that the U.S. government would need to request Ireland's assistance under the existing Mutual Legal Assistance Treaty (MLAT) between the two countries. *Microsoft* v. *United States*, 829 F.3d 197 (2d Cir. 2016). A divided court denied rehearing *en banc*, with several judges issuing lengthy and spirited opinions. *Microsoft* v. *United States*, 855 F.3d 53 (2d Cir. 2017). The U.S. government petitioned the Supreme Court for certiorari, which was granted on June 23, 2017.

The question the Supreme Court must answer is whether a probable-cause-based warrant issued under the SCA can reach digitally-stored materials within a provider's control, even if the provider has decided to store that material abroad. The government's primary argument is twofold: (1) Section 2703 of the SCA permits the government to require a U.S. service provider to disclose any electronic communication within its control; and (2) the disclosure of the contested information would take place within the United States, such that there is no question of extraterritoriality. Microsoft, for its part, contends that the physical location of the data should control, and that the SCA was not intended to apply to data stored in foreign countries. As such, a U.S. court cannot compel the company to disclose electronic communications stored abroad.

At oral argument on February 27, the parties and the justices wrestled with the fundamental question of how a statute drafted in 1986 intersects with the evolution of data storage technology.

The government, represented by Deputy Solicitor General Michael R. Dreeben, conceded that the SCA does not apply extraterritorially but emphasized the fact that the disclosure of the data from Microsoft to the government would take place within the United States. The government's primary point was that the latter instance falls within the "classically domestic conduct" covered by the SCA. Justices Sotomayor and Ginsburg questioned the government's distinction between the steps of obtaining and disclosing the information, noting that data necessarily would be located and collected abroad before being turned over in the United States. Justice Gorsuch weighed in here as well, asking the government how it could justify divorcing the two parts of the process. Justices Ginsburg and Sotomayor both asked questions as to whether the Court should maintain the status quo and leave it to Congress to amend the SCA or draft a new statute, especially in light of already pending legislation on the issue.[1]

Counsel for Microsoft argued that a warrant in this case would necessarily require extraterritorial action outside the scope of the SCA. In response, Justice Roberts commented that Microsoft was "assuming the answer to the question," as the government's position was that the disclosure at issue would be taking place within the United States. Justice Roberts expressed concern that if Microsoft were to prevail, companies would be able to attract customers by promising to shield data from government investigation via overseas storage. Justice Alito expressed a similar concern, positing a world where the government could show probable cause to obtain information in the emails of a U.S. citizen in connection with a crime that occurred within the U.S, but not be able to obtain the emails because the data is stored overseas by a U.S.-based company. In Justice Alito's view, this would require the government to deal with any number of bilateral treaties, delaying domestic criminal justice processes by months or years.

Justice Breyer appeared to be searching for a middle ground. He asked whether the statute as written would permit U.S. courts to issue warrants for data stored overseas, but allow companies like Microsoft to raise issues, including conflicts with foreign law, before the issuing judge. This may have been an appeal to Justice Kennedy, who expressed frustration with the "binary" choice between the location of the data and the location of the disclosure presented by the parties. Justice Kennedy asked whether other factors, such as where the owner of the email account lives or the location of the service provider's headquarters, should come into play.

[1] Recently, a bipartisan group of lawmakers introduced legislation called the CLOUD Act, which would permit warrants for data stored overseas, but would give service providers and the countries where the data is stored a chance to object to these disclosures.

It is not at all clear how the justices will rule in this case, but it is likely that the Court will hand down a decision by the end of June 2018. In addition, it remains uncertain how the timing of the decision will correlate with the progress of the CLOUD Act in Congress and any other legislation on this issue that may be proposed.

* * *

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

Amy L. Barton
+1-212-373-3285
abarton@paulweiss.com

E-Discovery Counsel Ross M. Gotler, E-Discovery Attorney Lidia Kekis and Associate Rebecca Orel contributed to this Client Memorandum.