October 19, 2017

In *Microsoft*, U.S. Supreme Court Will Review Extraterritorial Reach of Search Warrants

On October 16, 2017, the U.S. Supreme Court granted certiorari in *United States* v. *Microsoft Corp.*, U.S., No. 17-2, a high profile case that may have far-reaching impact on how and where U.S. companies store their customers' electronic information.

In connection with a narcotics investigation, the U.S. government sought a warrant to obtain email content and information from a person's Microsoft Network (msn.com) email account. On December 4, 2013, after finding probable cause that the email account had been used in furtherance of the crime being investigated, Magistrate Judge James C. Francis of the Southern District of New York issued the requested warrant against Microsoft under the Stored Communications Act (SCA) section 2703.

Microsoft determined that some of the requested data responsive to the warrant was in a Microsoft data center located in Dublin, Ireland. On December 18, 2013, Microsoft moved to quash the warrant to the extent it sought responsive email content stored in Ireland, arguing that U.S. courts do not have authority to issue SCA warrants for extraterritorial search and seizures and that collecting the information would violate Ireland's data protection laws.

In *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), Judge Francis denied Microsoft's motion, explaining, "Although section 2703(a) uses the term 'warrant' and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the [Internet Service Provider] in possession of the information and does not involve government agents entering the premises of the [Internet Service Provider] to search its servers and seize the e-mail account in question." Microsoft appealed and, on July 31, 2014, after hearing oral arguments, District Judge Loretta Preska of the Southern District of New York adopted Judge Francis's conclusions and affirmed his ruling from the bench.

Microsoft appealed to the Court of Appeals for the Second Circuit, which reversed and remanded the case with instructions to quash the portion of the warrant instructing Microsoft to collect, import, and produce the person's email content stored abroad. *Microsoft Corp.* v. *United States*, 829 F.3d 197 (2d Cir. 2016). The Second Circuit held 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. On June 23, 2017, the U.S. government petitioned the U.S. Supreme Court for certiorari on the question "Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad."

In the meantime, various courts across the country deviated from the Second Circuit's reasoning, upholding similar warrants issued under the SCA. These decisions, including some involving warrants issued to Google, reasoned that the SCA warrant calls for a search, not a seizure, that occurs in the U.S., that the data is in the company's possession and control (regardless of physical location), that the invasions of privacy occur in the U.S., and that the SCA lacks clear expression of Congressional intent of extraterritorial application. In addition, both the House and the Senate held hearings on the issue, arguing that the best resolution may be Congress updating the law.

The Supreme Court's eventual decision in this matter could have a significant impact on how many U.S. companies, not just Microsoft, conduct business in this modern age. Companies regularly store information in locations around the world, often to help improve the user experience for customers, as being physically closer to their electronic information may improve the speed at which customers are able to access that information, which may include their email and other electronic documents. Indeed, during the course of this matter, many technology companies have filed amicus briefs in support of Microsoft. Companies including Apple, Cisco, Verizon, and AT&T have supported the argument that if the U.S. government is able to gain access to extraterritorial data in a manner that is contrary to U.S. and non-U.S. data privacy and protection laws, customer privacy would be compromised and there would be a significant detrimental impact on business.

The Supreme Court's decision in this matter is also certain to be watched with interest overseas, where there has been an increased focus on personal data privacy issues in light of the 2015 *Schrems* decision in the European Court of Justice that invalidated the U.S.-EU Safe Harbor Framework on cross-border information transfer over concerns regarding the reach of the U.S. government.

* * *

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

Daniel J. Toal
+1-212-373-3869
dtoal@paulweiss.com

Liza Velazquez
+1-212-373-3096
lvelazquez@paulweiss.com

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