Microsoft: Supreme Court Decision on Jurisdiction over Foreign-Located Communications Anticipated

Yesterday, the Supreme Court granted *certiorari* in *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.* (*Microsoft*). In taking the case for review, the Supreme Court has signaled that it will address a key unsettled question concerning the territorial reach of a warrant issued under the Stored Communications Act of 1986 (SCA or the Act). As the Fourth Amendment does not protect information voluntarily disclosed to a third party,[1] Congress passed the SCA to provide privacy protections to information stored electronically by third parties. The SCA authorizes law enforcement authorities to obtain a warrant to seize electronically stored information, communications, and other materials from a third party upon a showing of probable cause.[2] At issue is whether the reach of a warrant issued pursuant to the SCA is territorially limited to the United States like a conventional warrant. The case has significant implications for electronic service providers that maintain customer data and customers whose data is stored with Microsoft and other electronic service providers, as well as broader relevance to the extraterritorial reach of U.S. law enforcement tools and techniques.

Case Background

In December 2013, as part of a criminal narcotics investigation in the Southern District of New York, law enforcement authorities sought and obtained an SCA warrant authorizing the search and seizure of information including emails "associated with a specified web-based e-mail account" stored by Microsoft.[3] After receiving the SCA warrant, Microsoft determined that while some of the responsive information was stored on U.S. servers, customer emails sought by the warrant were stored on company servers located in Dublin, Ireland.[4] In response to the warrant, Microsoft turned over the U.S.-located data, but moved to quash the warrant to the extent it sought the production of information or documents stored abroad.

Under existing case law, courts do not have the authority to issue warrants that seek materials located outside of the United States without specific legislative authority or a jurisdictional basis for doing so. Law enforcement authorities must follow procedures prescribed by Mutual Legal Assistance Treaties to seize foreign-located materials. Some federal courts have held that if an entity is subject to the jurisdiction of the United States, a conventional subpoena can compel the production of documents in their custody or control regardless of location.[5]

Pursuant to the SCA, U.S. law enforcement authorities may obtain a warrant requiring an electronic service provider to produce third-party data such as customer information, emails, and other materials upon a showing of probable cause. The SCA also allows for the enforcement of subpoenas, but only if prior notice is given.[6] In seeking to quash the SCA warrant with respect to foreign-located data, including emails, of a specified but publicly undisclosed customer of Microsoft that the company stored on servers in Ireland consistent with its standard storage practices, the company argued that because an SCA warrant is issued "using the procedures described in the Federal Rules of Criminal Procedure" like a conventional warrant, it is similarly territorially limited.[7]

A Southern District of New York magistrate judge disagreed. After conceding that SCA warrants are obtained using the same procedures as a conventional search warrant, the judge held that an SCA warrant is a hybrid law enforcement tool, part subpoena and part warrant. As a result, while the procedures for obtaining one are similar to those used to obtain a conventional warrant, the execution of an SCA warrant operates like a subpoena because it is "served on the [service provider] in possession of the information and does not involve government agents entering

Nicole H. Sprinzen

Vice Chair, White Collar Defense & Investigations

nsprinzen@cozen.com
Phone: (202) 471-3451
Fax: (202) 861-1905

Thomas Ingalls

Associate

tingalls@cozen.com
Phone: (202) 471-3411
Fax: (202) 861-1905

Related Practice Areas

- Appellate
- White Collar Defense & Investigations

premises of the [service provider] to search its servers and seize the email account" sought.[8] The court reasoned that SCA warrants thus do not implicate principles of extraterritoriality any more than traditional subpoenas and the SCA warrant requiring Microsoft to produce data from foreign-located servers was valid.[9] The district court affirmed the ruling and Microsoft appealed to the Second Circuit.

The Second Circuit reversed. In analyzing whether the presumption against extraterritorial application is overcome by the Act, the appellate court examined the history of the SCA, as well as its purpose of "protect[ing] a user's privacy interests."[10] Finding that "Congress did not intend[] the SCA's warrant provisions to apply extraterritorially,"[11] the court reversed the lower court's decision and quashed the warrant. The government appealed to the Supreme Court.

Split Among the Circuits

At the same time that *Microsoft* was making its way to the Supreme Court, district judges in the Third, Ninth, and D.C. Circuits hearing similar challenges by Google to SCA warrants have unanimously denied the company's motions to quash. In *In re Search of Content Stored at Premises Controlled by Google Inc.*, a federal judge in the Northern District of California ruled that because Google could obtain access to overseas-stored documents from its U.S. headquarters, it could be forced to comply with the SCA warrant.[12] Additionally, the court found that because the SCA warrant could be properly characterized as involving "domestic execution," it could be enforced regardless of where the information was located.[13]

Likewise, in *In re Information Associated with [Redacted]@gmail.com,* a federal district court judge with the U.S. District Court for the District of Columbia affirmed a magistrate judge's ruling that Google must provide data to the Department of Justice because an SCA warrant "does not amount to an extraterritorial application of the SCA ...."[14] She opined that the Second Circuit "erred" and that "every other court to consider the issue ... has resolved this question differently and rejected the holding of *Microsoft*."[15] Focusing on the fact that the disclosure is sought and made in the U.S., the court ruled that an SCA warrant can require production of foreign-located documents and information.[16]

Most recently, a federal judge in the U.S. District Court for the Eastern District of Pennsylvania also rejected Google's efforts to quash a subpoena.[17] Again the court noted that the workings of an SCA warrant after it is obtained are "more closely analogous to the workings of subpoenas and court-ordered discovery" that conventionally can reach records in the possession or control of a party regardless of the location of the records.[18] Additionally, the court found that because the SCA warrant provision seeks to regulate a provider's disclosure of data to the government and that disclosure takes places in the United States, an SCA warrant is not limited to U.S.-located data.[19]

Significance of Supreme Court's Grant of Certiorari

The Supreme Court's grant of *certiorari* indicates a forthcoming decision on the specific question of whether law enforcement authorities can use the SCA to obtain a third party's foreign-stored electronic information under the SCA's warrant provision. The decision also will have implications relating to the broader question of the extraterritorial reach of U.S. process, which has become an area of developing jurisprudence. If the Court holds that documents and information stored overseas are subject to collection by an SCA warrant, an SCA warrant would function like a traditional warrant in terms of its procedure but would have unique and unprecedented reach. Alternatively, a ruling by the Supreme Court that Congress did not intend the SCA to apply extraterritorially would be a decisive direction to U.S. law enforcement concerning the limits of document and information collection authority. The outcome of this case thus has significant implications regarding the bounds of law enforcement investigative efforts, users' privacy rights, and the obligations of electronic service providers and other companies that store user data.

Cozen O'Connor's White Collar Defense & Investigations attorneys are available to provide counsel and guidance on the issues discussed in this Alert.

---

[1] *See Smith v. Maryland*, 442 U.S. 735, 745-46 (1978).

[2] The SCA also allows authorities to require disclosure of third-party information via a subpoena, but it requires prior notice to the individual whose records are sought. 18 USC § 2703(b)(1)(B).

[3] I*n re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 446, 468 (S.D.N.Y. 2014).

[4] Microsoft, like many service providers, stores most of a user's data as close as possible to where the customer resides to improve service. In this case, a customer's location is determined based on the "country code" entered when the customer registered. Interestingly, Microsoft does not independently confirm the location information supplied by a customer. *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 203 (2d Cir. 2016).

[5] *See, e.g., Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983) ("The test for the production of documents is control, not location.").

[6] 18 USC § 2703(b)(1)(B).

[7] *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 446, 470 (S.D.N.Y. 2014).

[8] *Id.* at 471.

[9] *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 2014 U.S. Dist. LEXIS 133901 (S.D.N.Y. Aug. 29, 2014).

[10] *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 222 (2d Cir. 2016).

[11] *Id.*

[12] *In re Search of Content Stored at Premises Controlled by Google Inc.*, 2017 U.S. Dist. LEXIS 129068 (N.D. Cal. Aug. 14, 2017).

[13] *Id.* at *6.

[14] *In re Information Associated with [Redacted]@gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *13 (D.D.C. June 2, 2017).

[15] *Id.*

[16] *Id.* at *68-74.

[17] *In re Search Warrant No. 16-960-M-1*, 2017 U.S. Dist. LEXIS 131230 (E.D. Pa. Aug. 17, 2017).

[18] *Id.* at *20-21.

[19] *Id.* at *24-25