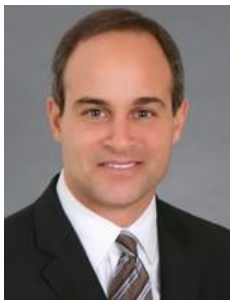
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# How 2nd Circ. Microsoft Ruling Will Affect Law Enforcement

*Law360, New York (July 26, 2016, 3:52 PM ET) --*


Grant P. Fondo

The Second Circuit recently issued a significant decision providing an important victory for technology companies, privacy advocates and those concerned with government overreach. In Microsoft Corp. v. U.S., 14-2985 (July 14, 2016), the Second Circuit held that the U.S. government had no authority under the Stored Communications Act to use a warrant to access data stored overseas. Importantly, it held that the proper nexus for jurisdiction over the storage of data is where the data is stored, rather than the location of the service provider or the data's owner. The decision also re-emphasizes the federal courts' continuing concerns as to the privacy implications of user's data and the government's efforts to gain access to it. And, it made law enforcement's efforts more difficult.

The case examined whether the SCA, 18 U.S.C. §§ 2701 et seq., permitted the government to use the act's warrant provisions to require a U.S.-based company to produce data stored abroad. The Second Circuit, in a 3-0 decision, held that Congress, in enacting the SCA, did so to enhance a user's privacy rights, rather than provide the government another tool for disclosure of information, and did not intend to expand the extraterritorial reach of search warrants. It held that § 2703 of the SCA "does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers." The decision overruled the magistrate court and district court's ruling requiring Microsoft to produce the data on the grounds that the operative nexus is control over the data, not the location of that data.

**The Data, Warrant and Microsoft's Motion to Quash**

This controversy began when the U.S. Attorney's Office for the Southern District of New York obtained a warrant pursuant to the SCA to obtain email data held and controlled by service provider Microsoft. The government sought the information in regards to a drug trafficking investigation. Microsoft produced the requested information to the extent it was located in the United States, but moved to quash the warrant to the extent it was seeking the Microsoft customer's email account stored outside the United States.[1] Specifically, while the data was located in a subsidiary's servers in Dublin, Ireland, it could be retrieved by Microsoft from the United States, and reviewed in the United States.

U.S. Magistrate Judge James C. Francis denied Microsoft's motion. In doing so, he referred to the fact that the SCA warrant is served on a service provider rather than on a law enforcement officer. Therefore, it "is executed like a subpoena in that it ... does not involve government agents entering the premises of the ISP to search its serves and seize the e-mail account in question." The magistrate judge

also found that the location of significance was where the government would review the content rather than the location of the data, and expressed concern about the practical consequents of precluding the government from accessing data stored off-shore. Microsoft appealed the ruling to the district court. There, Chief Judge Loretta A. Preska adopted the magistrate judge's reasoning and affirmed his order denying Microsoft's motion to quash. Microsoft then appealed to the Second Circuit.

**The Parties' Contentions**

Microsoft, in its appeal, asserted that the SCA's use of the term "warrant" meant what it said, in that the tool being used by the government was a warrant, and that court issued warrants carry territorial limitations, i.e., limiting the seizure of items (in this case, data) to the United States. The government, in contrast, asserted the jurisdictional nexus is not where the documents are located, as long as the holder of the documents, located in the U.S., can extract the data. It further asserted that the term "warrant" as used in the SCA is more akin to a subpoena, which does not have the same jurisdictional limitations as a traditional warrant under Rule 41.

**Ruling**

The Second Circuit, in ruling for Microsoft and overturning the district court's decision, examined two primary issues. First, whether Congress intended to have the warrant provisions of the SCA reach outside of the United States. Second, if the answer was no, whether the enforcement of the warrant constituted an unlawful extraterritorial application of the SCA. In examining these issues, the Second Circuit made a number of holdings that are likely to have a significant impact on the scope of privacy protections and government investigations.

As to whether the SCA specifically refers to an extraterritorial reach, both parties agreed that there is no specific language in the SCA that provided for extraterritoriality. And the Second Circuit found none. Consequently, under Morrison v. National Australian Bank Ltd., 561 U.S. 247 (2010), the Second Circuit confirmed that there is a presumption against the extraterritoriality reaches of the government.

The Second Circuit further found instructive the SCA's use of the term "warrant." The term "warrant," embedded in the Fourth Amendment in the U.S. Constitution, acts to address and limit searches and seizures in the United States. In examining the SCA, the Second Circuit found that warrants and subpoenas are distinct, and that the SCA treats these instruments as such pursuant to § 2703, in that basic subscriber data may be obtained via a subpoena, whereas a warrant is required to obtain email content. Thus, the Second Circuit rejected the government's argument that the structure of the SCA is such that the SCA's "warrant" is more akin to a hybrid of a traditional subpoena and warrant. Further, the Second Circuit noted that courts, in assessing the reach of subpoenas, have not compelled a third party, holding another's property, to produce the property if it is off-shore. Consequently, the Court found that the SCA does not permit the application of its warrant provisions to apply extraterritorially.

Given this holding, the Second Circuit then examined whether the focus of the SCA warrant provisions are such that the domestic contacts presented by the case "fall within the 'focus' of the statutory provision or are the 'objects of the statute's solicitude.'" The court found that the SCA's focus is user privacy — protecting the third-party user's stored electronic communications. In reaching this conclusion, it rejected the government's assertion that the SCA's purpose, in providing the various mechanisms to obtain user data, was "disclosure." The Second Circuit found that the intent in enacting the SCA was to enhance the privacy protections for users of service providers. Citing the legislative history, the Second Circuit found "Congress sought to ensure the protections traditionally afforded by

the Fourth Amendment extended to the electronic forum."

Having determined that the SCA's focus is privacy rather than disclosure, the court had "little trouble" finding "that the execution of the Warrant would constitute an unlawful extraterritorial application of the [SCA]." The data was located in Dublin, Ireland, and would have to be seized from that location. Thus, content subject to the warrant is off-shore, and would be seized by a third-party, Microsoft, for and acting as an agent of the government. Importantly, the Second Circuit found that the user's location was irrelevant (and often unknown to law enforcement) to its analysis, as was the location of the service provider.

The Second Circuit rejected the government's concerns that this ruling would place a substantial burden on the government in seeking data for its investigations, finding that the burden did not supersede the SCA's limitations on the use of warrants.

**The Government's Options**

The government has the following options, none of which have a high degree of success. First, it can request the entire Second Circuit review the matter, referred to as seeking en banc review. This is unlikely, as this type of request is infrequently granted, particularly where the vote is 3-0.

Second, the government can request the U.S. Supreme Court grant a writ of certiorari, requesting the Supreme Court review and reverse the decision. In order to do so, the U.S. Attorney's Office in the Southern District of New York must first obtain the permission of the U.S. Solicitor General's Office to seek cert. Although this is an important and impactful decision, it is not a forgone conclusion that permission will be granted. The Solicitor General's Office is strategic about which cases it appeals, and will only do so where there is an important issue at stake, and it believes the circuit court got it wrong. Even if the Solicitor General's Office agrees to appeal the decision, the likelihood the Supreme Court will grant cert. is low.

Third, the U.S. Department of Justice can request Congress amend the statute. While extremely difficult to convince Congress to rewrite legislation, it is possible particularly if there is a significant movement of data off-shore as a result of this decision. Currently, there is heightened terrorism and domestic safety concerns, and there can be little doubt that this ruling will slow down investigations involving data stored off-shore. Further, obtaining data from foreign countries may prove difficult. Currently, U.S. law enforcement seeks evidence abroad through the mechanisms provided by mutual legal assistance treaties, which are between the U.S. and other countries. Not every country has entered into a MLAT with the U.S., and for those that have they do not all consider U.S. law enforcement's requests a high priority, or have efficient mechanisms to obtain the requested information. The delays will only get worse given what is likely to be an increase in these requests.

**Practical Ramifications**

This case is a significant victory for privacy advocates, technology companies and those concerned with government overreach. It also continues the federal courts' trend in protecting digital privacy, following cases such as Riley v. California, 573 U.S. 1 (2014), in which the Supreme Court held that the government must obtain a search warrant to seize and search data on a smart phone.

The government was correct that this ruling will make it more difficult and time-consuming for law enforcement to obtain information. Given this ruling, law enforcement will be required to seek foreign

assistance for data stored off-shore, and there is no question that the MLAT process is a slower and more laborious process. Further, not all countries adhere to the MLAT process, thus precluding the government from getting data that it previously could have obtained. Law enforcement may also forgo even attempting to get off-shore data that it might have previously sought, due to the delay and aggravation. Given the impact of this decision, it seems likely that the government will seriously evaluate seeking a reversal of this decision.

In the interim, this ruling will only further incentivize companies to store data off-shore, both in the context of reducing compliance costs (which are significant) and protecting their users' data from U.S. law enforcement seeking access to it.

—By Grant P. Fondo, Goodwin Procter LLP

*Grant Fondo, a former assistant U.S. attorney in the Northern District of California, is a partner in Goodwin Procter's Silicon Valley and San Francisco offices and co-chairman of the firm's blockchain and digital currency practice.*



[1] Order, p. 1