

Certiorari Grant This Week on Email Providers Served with Warrant for Emails

by Edward B. Magarian and John Marti

The Internet has not only become a backbone for social and business commerce, but, it has become a vehicle to pursue nefarious purposes. Law enforcement and intelligence agencies, believing that material evidence is located outside the United States, seek to hold U.S. companies, with foreign operations, responsible for producing that evidence to the government in the United States. In those cases, the U.S. government often maintains that evidence is within the control of and accessible by U.S. companies no matter where the evidence is located. The tension between individual privacy interests and governmental interests in security and foreign sovereignty is raising its head once again, this time before the Supreme Court of the United States.

On Monday, October 16, 2017, the Supreme Court, in a case which raises the broader question of how hard federal and state governments can push to obtain evidence hosted abroad, agreed to take up the specific issue of “[w]hether 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.” U.S. Supreme Court Docket, 17-2 *United States v. Microsoft Corporation*, available at <https://www.supremecourt.gov/qp/17-00002qp.pdf>. The issue arises from the United States’ petition for a writ of certiorari in *United States v. Microsoft Corp.*, Sup. Ct. No. 17-2, where the Second Circuit “conclude[d] that Congress did not intend the [Stored Communications Act’s] SCA’s warrant provisions to apply extraterritorially.” *Microsoft Corp. v. United States*, 829 F.3d 197, 222 (2d Cir. 2016).

The issue in this case concerned a warrant directed at Microsoft, requiring it to seize and produce the email contents for a Microsoft customer who uses a Microsoft email account, and was believed to do so in furtherance of narcotics trafficking. *Id.* at 200. Microsoft produced its non-content information that was stored in the United States, but moved to quash the warrant as to the customer content, which was stored and maintained in Ireland. The challenge pitted Microsoft’s view of a warrant as traditionally having territorial limitations, against the government’s view that this was simply an extension of

Related People

- Edward B. Magarian
- John Marti

Related Capabilities

- Government Enforcement & Corporate Investigations
- Appellate

the principle requiring production of documents within the corporation's "custody or control." *Id.* at 201. The district court found for the government, denied the motion to quash, and held Microsoft in contempt of court. *Id.* The Second Circuit, however, reversed, vacated, and remanded, employing a statutory interpretation analysis as to the territorial reach of the SCA. *Id.* at 205-222. Judge Lynch, writing separately, "concur[re]d in the result, but without any illusion that the result should even be regarded a rational policy outcome, let alone celebrated as a milestone in protecting policy." *Id.* at 222-33 (Lynch, J., *concurring in the judgment*).

The Second Circuit's reversal prompted the United States to petition the Supreme Court for a writ of certiorari. The United States' petition cited a broad conflict with the Supreme Court's guidance in interpreting a statute's extraterritorial scope, as well as a conflict with the law from the federal courts of appeals as to the scope of subpoenas, which can reach documents outside the United States. Petition for a Writ of Certiorari at 21-25, available at <http://www.scotusblog.com/wp-content/uploads/2017/07/17-2-petition.pdf>. The Petition also emphasized that the Second Circuit's holding compromised the safety and security of Americans by hampering not only the government's ability to prosecute crimes, but also to fight off terrorism and national security threats. *Id.* at 26.

The importance of this issue to governments at both the federal and state level is highlighted by the amicus brief filed in support of the United States by 33 States (and Puerto Rico). Amicus Brief, available at <http://www.scotusblog.com/wp-content/uploads/2017/08/17-2-tsac-states-of-vermont.pdf>. While the Second Circuit focused on the statutory language of the Stored Communications Act, a decision by the Supreme Court may implicate broader concerns, and raise significant implications for corporations served with subpoenas for evidence in the possession of their foreign corporations or vendors, both of which may be subject to potentially competing laws. For example, European nations often object to the United States' attempts to access data within their border. Yet, European law enforcement authorities continue to seek customer data from American technology companies, and to impose European data privacy principles to data hosted by U.S. companies abroad. Other sovereigns, including China and Russia, seek to control and exploit customer data hosted inside their territorial borders, as well as attempt to leverage U.S. companies hosting data both locally and abroad.

Although no amicus support for Microsoft was filed at the petition stage, strong amicus support for Microsoft is expected once the case is briefed on the merits. Oral argument for this case has not been set, but can be expected for early 2018, with an opinion issued by the end of June 2018.