

Location, Location, Location: Microsoft Debate Over Government's Access to Overseas Data Heads to the Supreme Court

Minding Your Business Blog on **October 26, 2017**

On October 16, 2017, the Supreme Court agreed to review the Second Circuit's decision in [United States v. Microsoft Corp.](#), a case that highlights the current tension between law enforcement needs and privacy concerns in a rapidly changing digital landscape.

The dispute between Microsoft and the government arose when Microsoft refused to comply with a warrant that would have required Microsoft to disclose information about an e-mail account which the federal government believed was being used for drug trafficking. A federal magistrate judge issued the warrant under 18 U.S.C. § 2703, the Stored Communications Act ("SCA"), which is part of the Electronic Communications Privacy Act of 1986 ("ECPA"). The SCA gives the government the authority to require a provider of an electronic communication service or remote computing service to disclose content and non-content information about a wire or electronic communication. Though Microsoft—a U.S. based company—was served at its headquarters in Washington State, the company refused to provide the requested content because it had migrated the e-mails in question to a data-center in Ireland. Microsoft argued that because the data was now located overseas, the e-mails were outside the government's reach and beyond the scope of the SCA—despite the fact that, using a computer program, Microsoft could access and migrate the e-mails back to the United States.

Microsoft moved to quash the warrant, arguing that it constituted an impermissible extraterritorial application of the SCA. The magistrate judge was unpersuaded, noting that the SCA did not alter the basic principle that, when it comes to subpoenas, an entity that is obligated to produce to the government any information in its control must do so—regardless of the location of the information. Though the district court affirmed the decision to uphold the validity of the warrant, a panel of judges in the Second Circuit Court of Appeals reversed. The panel reasoned that the focus of the SCA was the protection of privacy, noting that any invasion of privacy would occur where the data was physically located. Therefore, the panel held that the government was not authorized to enforce SCA warrants against U.S.-based service providers if the data in question was stored overseas.

As both the United States and Microsoft acknowledged in their briefs to the Court, there currently exists no circuit split to prompt the Court’s intervention, but the high stakes surrounding the case cannot be overstated. As [Microsoft argued in opposition](#) to the petition for certiorari, the case implicates numerous privacy and technology-related concerns, such as “the interest in maintaining protections commensurate with the public’s privacy expectations for our most personal communications and documents; the dangers of infringing foreign sovereignty by unilaterally seizing personal communications data from a foreign country . . . and the adverse effects the U.S. technology sector will suffer if it becomes the conduit through which U.S. law enforcement can seize the private communications” of every U.S. service provider’s customers, regardless of where the customers or their data is located. But as [the government argued in its reply brief](#), under the Second Circuit’s ruling, “hundreds if not thousands of investigations of crimes—ranging from terrorism, to child pornography, to fraud—are being or will be hampered by the government’s inability to obtain electronic evidence.”

One final question that looms in the background of this clash between law enforcement and privacy advocates, which was raised by Microsoft in its opposition, is whether the Supreme Court is the proper forum for this debate, given that the Justices are confronted with an “all or nothing” choice—either the government can use the SCA to compel disclosure of all overseas data under U.S. control, or it cannot compel the production of any overseas data simply because of where it is located. As Joshua Newville and Lindsey Olson discussed in a [previous blog post on the Second Circuit’s ruling in the *Microsoft* case](#), and in [a recent New York Law Journal article](#), there have been discussions in Congress about possible bipartisan amendments to the ECPA to resolve the challenges that come from trying to apply a 20th century law to 21st century technology. Perhaps in making a ruling on the scope of the SCA as it is currently written, the Supreme Court will provide Congress with a clearer path on how to amend the statute and strike a better balance between the government’s legitimate investigative needs and the public’s privacy expectations.

[View Original](#)