New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 83
MONDAY, OCTOBER 30, 2017

INTERNATIONAL CRIMINAL LAW AND ENFORCEMENT

Expert Analysis

# Battle Over Emails Stored Overseas Reaches Supreme Court

By **Philip Patterson** And **Vera Kachnowski**

The extraterritorial reach of U.S. law enforcement will face scrutiny once more, with the Supreme Court granting certiorari this month in the highly-publicized—and hotly-contested—dispute over a warrant for Microsoft emails stored on a foreign server. *United States v. Microsoft*, No. 17-2 (cert. granted Oct. 16, 2017). The case highlights a recurring tension between public safety and privacy concerns, and underscores the increasing complexity behind the technology we all rely on each day.

In the last round of the Microsoft saga, a Second Circuit panel reversed the district court and quashed a warrant for emails of a criminal suspect that were stored on a Dublin server. *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016) (*Microsoft*). The panel concluded that execution of the warrant would involve an impermissible extraterritorial application of the Stored Communications Act (SCA). Nearly 90 amici, including technology and media companies, civil liberties groups, and governments, had submitted briefs to the circuit and its decision was divisive, even internally: An en banc rehearing was denied by a split 4-4 vote, with strong dissents questioning the merits and implications of the original opinion. *Microsoft v. United States*, 14-2985 (2d Cir. Jan. 24, 2017). All called for a legislative fix.

Since then, Congress held hearings on law enforcement access to foreign-stored data, but no other circuit court reached the issue. (Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing before the S. Judiciary Subcomm. on Crime and Terrorism (May 24, 2017); Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing before the H. Judiciary Comm. (June 15, 2017)). The various district courts that addressed it, however, roundly disagreed with the Second Circuit's ruling. According to the government's petition, service providers are nonetheless resisting SCA warrants based on *Microsoft*, impeding law enforcement and public safety. While legislative efforts may continue in parallel, the Supreme Court appears to agree that urgency exists to hear the dispute now, even in the absence of a formal circuit split.

## Background

At issue is §2703 of the SCA, a multi-provision statute that is part of the Electronic Communications Privacy Act of 1986. 18 U.S.C. §§2701-2712. The SCA generally affords Fourth Amendment-like protections to electronic communications and prohibits unauthorized access to or disclosure of such information. Section 2703, however, permits the government to use warrants, subpoenas, or court

PHILIP PATTERSON AND VERA KACHNOWSKI *practice white-collar criminal defense and international investigations at De Feis O'Connell & Rose, P.C., a Manhattan law firm.*

orders to compel disclosure from service providers. Of these options, the government is required to obtain a warrant, on a probable cause showing, for communications stored for less than 180 days. The government can also use a warrant for longer-stored data or else seek such data by subpoena, but only with notice to the accountholder. 18 U.S.C. §2703.

The service provider here—Microsoft—was served with a §2703 warrant at its U.S. headquarters for "content" and "non-content" information about an email accountholder. As is increasingly common, Microsoft had procedures in place to optimize efficiency by breaking up the electronic account data and storing it in different physical locations. Most of the data, including the content of the emails, automatically migrated to a server in Dublin because the accountholder inputted the country code for Ireland. The email contents could, however, be "collected" and viewed by certain Microsoft employees in the United States.

> The case highlights a recurring tension between public safety and privacy concerns, and underscores the increasing complexity behind the technology we all rely on each day.

Microsoft moved to quash the warrant for the Dublin-stored data on the grounds that it would constitute an impermissible extraterritorial search and seizure. The magistrate judge denied Microsoft's motion, and the district court affirmed. On appeal, the circuit quashed the warrant, and the government's writ petition followed.

### Questions for the Court

The court's review will begin with at least one area of agreement between the parties: Section 2703 does not provide for extraterritorial application. Indeed, U.S. statutes are presumed not to apply extraterritorially unless otherwise indicated, and the presumption has not been rebutted here. *Morrison v. National Australian Bank*, 561 U.S. 247 (2010). The court instead will evaluate whether, as the government contends, the Microsoft warrant involves a permissible domestic application of the statute. That question turns on the statute's focus, and whether the conduct relevant to that focus occurred within the United States. *RJR Nabisco v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016).

The SCA's focus is disputed. The circuit held that the language of the SCA and its legislative history make clear that its focus is *privacy,* and that the relevant conduct is Microsoft's accessing data located in Ireland. The government's petition agrees that certain SCA provisions address privacy, but contends that §2703's focus is *disclosure*, namely "disclosure in the United States of information that the provider can access domestically with the click of a computer mouse." The government contends that even if §2703's focus was privacy, the domestic disclosures are still the relevant conduct; Microsoft does not violate its users' privacy by internally accessing their data. In any case, the government maintains that privacy interests are protected by the warrant's probable cause requirement. Petition for Writ of Certiorari (Petition), at 12, 17, 31.

The very nature of §2703 warrants is also disputed. The magistrate and district judge concluded that SCA warrants, despite their name and probable cause requirements, function more like subpoenas: they require service providers, rather than law enforcement, to gather the requested materials. Subpoena law requires recipients under U.S. jurisdiction to produce information in their possession, custody, and control regardless of its location, leading the lower courts to enforce the Microsoft warrant. On appeal, the circuit held that §2703 clearly distinguishes between subpoenas and warrants, and noted that warrants have "distinctly territorial" limitations. Moreover, the circuit noted that "our Court has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy

interest in the item." *Microsoft*, 829 F.3d at 212-16 (citation omitted).

### Whose Data Is It Anyway?

In the government's view, service providers "control" all accountholder data and must produce requested data regardless of where they choose to store it. But as the circuit noted, such service providers may be more like "caretakers" of data and bound to consider the underlying accountholder's separate privacy interest. The scope of that interest, in turn, may depend on the identity of the particular user. As the circuit observed, the record is silent on the location and nationality of the Microsoft user who sparked all this litigation. But such details may matter as the court (and Congress) assess these issues.

For example, in a joint *amicus* brief supporting the government's petition, thirty-three states and Puerto Rico represented that service providers have refused to comply with SCA warrants post-*Microsoft* "even when (1) a court has found probable cause that the email account was used in connection with a domestic crime, (2) the provider can access the requested data from within the United States, and (3) *the suspect and the provider are both in the United States*." Brief Amici Curiae of the States of Vermont, et al. in Support of Petitioner, at 3 (emphasis added). In its petition, the government made a similar representation, noting that the "harmful effects of the panel's decision [] extend beyond investigations involving the email of foreign nationals." The government added that the *Microsoft* decision "provides a roadmap for terrorists and criminals in the United States to insulate electronic communications from U.S. investigators—they need do nothing more than falsely state a location outside the United States when signing up for an account." Petition, at 27.

It seems unlikely that Congress intended such a result or foresaw it, given the vastly different technology that existed at the SCA's 1986 passage. The analysis is muddier, however, as to foreign residents and nationals, given traditional warrants' territorial limits and the potential tensions between U.S. and foreign laws, especially on privacy. Perhaps a starting point, as some have suggested, is to focus on users' nationality and residence, rather than the location of their data, which may be unconnected for business or technological reasons. *See, e.g.,* Testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google.

All eyes will be on the Supreme Court as they review the thorny Microsoft issues anew.

### Conclusion

Stakeholders affected by the *Microsoft* decision agree that serious competing policy considerations must be weighed to align the SCA with modern technology and the increasing importance of digital evidence to law enforcement—not just in the United States, but worldwide. Indeed, any legislative remedies must take into account the parallel data requests made by foreign governments and the potentially conflicting international compliance demanded of service providers. In the meantime, all eyes will be on the Supreme Court as they review the thorny Microsoft issues anew.