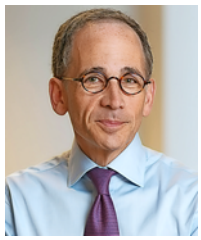
Bloomberg BNA

Privacy and Security Law Report®

Microsoft v. U.S.

In *Microsoft Corp. v. U.S.*, the U.S. Court of Appeals for the Second Circuit ruled that American companies can't be forced to turn over the content of a customer's e-mail stored in an overseas data center to U.S. law enforcement. The decision highlights the fact that the status quo is no longer tenable—and judges bound by outdated laws are ill-equipped to solve such modern problems, the authors write.

Microsoft v. United States: A Journey Into the Cloud



BY CRAIG A. NEWMAN

The law, it seems, is forever chasing technology.

And last week, a federal appeals court ruling underscored the vexing challenges created when data flows seamlessly across international borders and is stored in data centers around the world. In *Microsoft Corp. v. U.S.*, the U.S. Court of Appeals for the Second Circuit ruled that American companies can't be forced to turn over the content of a customer's e-mail stored in an overseas data center to U.S. law enforcement. *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.*, 2d Cir., No. 14-02985, order, 7/14/16 (15 PVLR 1465, 7/18/16). The court held that a provision of an electronic communications law enacted 30-years ago, the Stored Communications Act (SCA), doesn't permit U.S. courts to enforce warrants beyond American soil.

The decision has far-reaching legal, diplomatic and practical implications for the global movement and storage of digital data and helps shape the broader debate about international privacy rights, technology and security. Up until a few years ago, tech giants like Microsoft Corp. stored data on U.S. servers so courts didn't question whether they were on firm ground in issuing warrants. But that has changed. U.S. companies increasingly host mountains of customer data around the world.

''Three decades ago,'' the court observed, ''international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st-century demands for access and speed and their related, evolving expectations of privacy.''

Craig A. Newman is a litigation partner at Patterson Belknap Webb & Tyler LLP in New York and chair of the firm's Privacy and Data Security practice. He represents public and private companies, professional service firms, non-profit institutions and their boards in litigation, governance and data security matters.

The views and opinions expressed in this article are those of the author and don't necessarily represent those of Patterson Belknap Webb & Tyler LLP or its clients.

Background: The First Two Rounds

Microsoft's tussle with the U.S. government started in December 2013 when a federal magistrate issued a seemingly routine warrant in a narcotics investigation—after making a ''probable cause'' finding—demanding

 ISSN 1538-3423

that Microsoft turn over messages from a customer's e-mail account. Law enforcement requests like this are made all the time and internet service providers typically comply. But this was different. The warrant sought e-mail not only stored on Microsoft's U.S. servers, but at one of its data centers in Dublin, Ireland, more than 4,500 miles from the company's Redmond, Wash. headquarters.

The decision has far-reaching legal, diplomatic and practical implications for the global movement and storage of digital data and helps shape the broader debate about international privacy rights, technology and security.

When Microsoft received the SCA warrant, its Global Criminal Compliance team determined that it would comply in part by producing the account information stored on servers located within the U.S., but would move to vacate the warrant to the extent it sought customer information stored outside the U.S. Because of sophisticated computer technology, Microsoft in the U.S. is able to access information stored on its servers from around the world.

Section 2703(a) of the SCA, enacted in 1986 as part of the Electronic Communications Privacy Act, says:

> A government entity may require the disclosure by a provider of electronic communications service of the contents of a wire or electronic communications, that is in electronic storage in an electronic communications systems for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction[.]

Throughout the case, Microsoft has read the statute as prohibiting the application of an SCA warrant outside of the U.S., a position the Second Circuit ultimately embraced. The SCA provides that a warrant must be issued ''using the procedures described in the Federal Rules of Criminal Procedure.'' Rule 41 of the Federal Rules of Criminal Procedure states that ''[f]ederal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States. . . .''

Microsoft lost the first two rounds of its fight with the government. In April 2014, a federal magistrate denied Microsoft's motion to vacate the warrant, ruling that an SCA warrant ''is a hybrid: part search warrant and part subpoena,'' and as such, functions more as a subpoena because it is merely served on an internet service provider—with the onus shifting to the recipient to look for responsive materials within its possession, custody or control and turn them over . The magistrate reasoned that a SCA warrant does not require the government to enter a company's premises and conduct a physical search and seizure that would be governed by Fourth Amendment protections. Then, in July 2014, U.S. District Judge Loretta Preska affirmed the magistrate's order from the bench, holding that the key issue was one of control over the user's information and not its physical location (13 PVLR 1416, 8/11/14).

The Second Circuit's Ruling

In a unanimous ruling, the three-judge panel held that a warrant issued under the SCA is governed by the location of the data sought. Because the e-mail was stored outside the U.S.—whether belonging to a U.S. citizen or foreigner—it is not subject to compelled disclosure under an SCA warrant.

''Because the content subject to the warrant is located in, and would be seized from, the Dublin data center,'' wrote Judge Susan Carney on behalf of the court, ''the conduct that falls within the focus of the [SCA] would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.'' The court found that ''Congress did not intend the SCA's warrant requirements to apply extraterritorially. . . .''

''[I]t is our view,'' the court said, ''that the invasion of the customer's privacy takes place . . . where the customer's protect[ed] content is accessed—here, it is seized by Microsoft, acting as an agent of the government.''

The court's analysis focused squarely on the legal presumption against the extraterritorial application of U.S. law and concluded that the SCA's warrant provisions do not contemplate or permit extraterritoriality. Indeed, the government conceded as much during oral argument. ''When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act,'' the court said, ''its aim was to protect user privacy in the context of new technology that required a user's interaction with a service providers . . . . Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas.''

Underlying the court's analysis are several other concerns:

Dueling Privacy Regimes

Microsoft urged the court to interpret the SCA in a way that ''creates the least international discord[,]'' and that by affirming the lower court rulings, it risked setting off ''global chaos'' and encouraging other nations to enact SCA-type laws, which would open the door to requiring companies in the U.S. to turn over customer information including that belonging to American citizens. During oral argument, Judge Carney pressed the government on this point, asking whether ''a German court requiring disclosure of a provider in Germany, regardless of where its servers are kept or who it's providing service to, can require the disclosure to happen there and U.S. customers or users can be effected but it should be of no concern to us. Is that right?'' The government conceded that it should be of ''some concern'' but that, under principles of international law, it was the ''norm.''

In the ruling, Judge Carney noted that ''[o]ur conclusion today serves the interests of comity that . . . ordinary govern the conduct of cross-border criminal investigations . . . [and] we find it difficult to dismiss [comity] interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States

  PVLR ISSN 1538-3423

judge issues an order requiring a service provider to 'collect' from servers located overseas and 'import' into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States.''

The ruling validates the current legal process for law enforcement and intelligence agencies to access information that resides in foreign data centers.

Had the court decided differently, it would have left cloud providers between a proverbial rock and hard place—not knowing whether to comply with a U.S. warrant or risk violating the law of where the data resides. For the moment, that issue is off the table, although will resurface if the government seeks rehearing or takes the case to the U.S. Supreme Court.

Mutual Legal Assistance Treaties

The ruling validates the current legal process for law enforcement and intelligence agencies to access information that resides in foreign data centers. The process—called a mutual legal assistance treaty or MLAT—typically requires the requesting government to comply with the other government's laws. For instance, Irish law requires authorization from an Irish judge to obtain e-mail content from a provider. This process wasn't used in *Microsoft*, perhaps because a 2013 report found that the MLAT process is ''too slow and cumbersome,'' taking an average of ten months.

Judge Gerald E. Lynch wrote a separate concurring opinion to highlight what, in his view, was at stake in the case. ''[T]he sole issue involved is whether Microsoft can thwart the government's otherwise justified demand for emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country.'' Further, he wrote that the dispute ''is not about privacy, but rather about the international reach of American law.'' And the decision about whether and when to apply U.S. law to actions abroad ''is left entirely to Congress'' and called upon them to ''revise a badly outdated statute.''

It's unlikely that the Second Circuit's ruling is the final word.

Reaction to the ruling was swift. Brad Smith, Microsoft's President and Chief Legal Officer said ''[i]t ensures that people's privacy rights are protected by the laws of their own countries; it helps ensure that the legal protections of the physical world apply in the digital domain; and it paves the way for better solutions to address privacy and law enforcements needs.''

In a statement, a Justice Department spokesman called the decision disappointing and said that ''[l]awfully accessing information stored by American providers outside the United States quickly enough to act on evolving criminal or national security threats that impact public safety is crucial to fulfilling our mission to protect citizens and obtain justice for victims of crime.'' At the same, the Justice Department disclosed that the White House is working on a legislative proposal to implement a bilateral agreement between the U.S. and U.K. that would permit U.S. companies to provide electronic data in response to U.K. orders targeting non-U.S. citizens located outside of the U.S. The proposal would give the U.S. reciprocal rights regarding data stored in the U.K. The proposal is in draft form and would require amending the SCA .

What's Next?

It's unlikely that the Second Circuit's ruling is the final word. The Justice Department has indicated that it is considering an appeal to the U.S. Supreme Court. It could also seek an en banc rehearing before the Second Circuit. But either way, the decision highlights the fact that the status quo is no longer tenable—and judges bound by outdated laws are ill-equipped to solve such modern problems.