New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 68
TUESDAY, OCTOBER 7, 2014

FEDERAL E-DISCOVERY

# Microsoft Paves the Way for Data Privacy Battle

By **H. Christopher Boehning** | And **Daniel J. Toal**

Microsoft Corporation has found itself at the center of an intense legal battle regarding the ability of the United States government to subpoena data stored abroad. In addition to drawing the attention of constitutional law scholars, technology companies, and lawmakers, the case has also implicated some emerging areas of e-discovery practice.

Microsoft stores messages sent and received by its email users at "datacenters." Although Microsoft does not disclose the exact number of datacenters it operates, the company confirms that there are between 10 and 100 worldwide.[1] The physical location of a user's data depends primarily on the proximity of that user to the various datacenters.

In December 2013, in connection with a narcotics investigation, Magistrate Judge James C. Francis of the Southern District of New York issued a search warrant related to a specific email account "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, Wash."[2]

Microsoft objected to the warrant to the extent that it sought information stored on servers at its datacenter in Dublin, Ireland. The company argued that the warrant requires a search and seizure outside of the United States and that complying with it would require Microsoft to violate Irish law. A legal battle ensued. On April 25, 2014, Francis denied Microsoft's motion to quash the warrant.[3] This ruling was upheld on July 31 by U.S. District Judge Loretta A. Preska of the Southern District of New York. Microsoft has since appealed to the U.S. Court of Appeals for the Second Circuit.

MICROSOFT

AN AERIAL view of Microsoft's data center in Dublin, Ireland

The importance of the case did not go unnoticed: Amicus briefs were filed on behalf of Microsoft by the Electronic Frontier Foundation and by technology companies including Verizon, AT&T, Cisco, and Apple,[4] with each of them arguing that customer privacy will be compromised if the U.S. government gains access to extraterritorial data. Verizon wrote that "if the Court were to permit the U.S. government to obtain, in a manner contrary to both U.S. and foreign law, customer data stored abroad, it would have an enormous detrimental impact on the international business of American companies, on international relations, and on privacy."[5]

The Department of Justice emphasized the significance of this case as well. In its brief opposing Microsoft's motion to vacate, the DOJ argued that Microsoft's position would dangerously undermine criminal investigations conducted by U.S. authorities.[6] If Microsoft succeeded on its motion to quash the warrant, the DOJ argued that service providers would be given excessive power to store and move information wherever they wanted. The DOJ also maintained that the physical location of the documents was irrelevant: The subject of the warrant was Microsoft itself, not the location where the data was stored.

H. CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* ROSS M. GOTLER, *e-discovery counsel, and* RAJ J. BORSELLINO, *an associate, assisted in the preparation of this article.*

### Constitutional Issues

The Microsoft battle implicates Fourth Amendment protection against unlawful searches and seizures. Microsoft General Counsel Brad Smith emphasized this point in a Wall Street Journal op-ed in July, calling attention to the case and arguing that the DOJ "seeks to sidestep" Fourth Amendment protections.[7]

Rules regarding compelled disclosure of electronic data are set by the Stored Communications Act (SCA), which was enacted as part of the Electronic Communications Privacy Act (ECPA) of 1986. In his ruling on the motion to quash, Francis noted that the SCA "was enacted at least in part in response to a recognition that the Fourth Amendment protections that apply in the physical world, and especially to one's home, might not apply to information communicated through the Internet."[8] Neither Microsoft nor the DOJ disputes that the SCA is steeped in Fourth Amendment protections, but they differed on whether the Fourth Amendment would be violated by the search warrant.

Microsoft and its supporting amicus briefs argued that the warrant "calls for the disclosure of content data that can only be obtained through an extraterritorial search and seizure."[9] Additionally, because Microsoft has so many datacenters worldwide, the company argued that the search warrant did not meet the Fourth Amendment's particularity requirement.[10] The language of the warrant required information that could be stored at any of Microsoft's worldwide locations, and did not name the Dublin datacenter as the specific location of the stored documents.

The DOJ countered by arguing that the SCA is not analogous to warrants that require search and seizure of physical evidence. Instead, SCA warrants are "the functional equivalent of a subpoena or other investigative demand on a service provider."[11] Francis agreed with the DOJ on its interpretation of the SCA search warrant. Referring to the warrant as "a hybrid: part search warrant and part subpoena,"[12] he determined that it is obtained like a search warrant but executed like a subpoena because it does not involve officers entering and seizing physical evidence. Therefore, Microsoft's objections regarding the physical location of the data were irrelevant.

### E-Discovery Issues

The Microsoft case highlights two key e-discovery topics for practitioners and companies, especially those with an international footprint: (1) it raises cross-border e-discovery and related issues such as international data privacy law and comity, and (2) it features questions regarding possession, custody, and control of data.

The Microsoft battle implicates Fourth Amendment protection against unlawful searches and seizures.

First, cross-border data transactions present difficult electronic discovery issues for companies. Although it is headquartered in the United States, Microsoft operates across the world and is subject to laws in many countries. The warrant issued by Francis put the company in a difficult situation: If it were to comply with Francis' warrant and produce data held at its Dublin datacenter, it could potentially violate Ireland's Data Protection Acts of 1988 and 2003. On the other hand, if it refused to comply with the warrant, it faced the prospect of being held in contempt of court. Microsoft chose the latter.

Different countries have differing notions of data protection and privacy, and the variance among laws can make cross-border electronic discovery especially difficult to navigate. An electronic file may be created in one country with strict data protection laws, and subsequently downloaded in another country that has no legal notion of data protection. There is little agreement among nations on how to address the conflict of laws.

Microsoft is not the first company to face such a conundrum. In *Linde v. Arab Bank*,[13] Jordan-based Arab Bank was ordered to provide the court with account records for customers located outside the United States. Arab Bank refused, claiming that the account records were protected by foreign bank secrecy laws in Jordan, Lebanon, and the Palestinian territories, and was thereafter sanctioned by the District Court for failing to disclose the records. The Second Circuit upheld the sanctions order on appeal, ruling that the interests of the United States government in disclosing the records outweighed the interests of the foreign governments in keeping them private. Arab Bank appealed to the U.S. Supreme Court earlier this year and was denied certiorari.

The Arab Bank case, as well as the district court's Microsoft ruling, demonstrates that judges prefer to enforce discovery in American courts and under American rules, even if it may be in conflict with other countries' laws. Practitioners should be aware of the increasing need to balance several sets of laws when engaging in litigations that involve electronic discovery in multiple nations.

Second, the Microsoft ruling raises questions of possession, custody, and control. Microsoft's primary claim in its motion to quash the subpoena was that the warrant sought information located outside the United States. Francis found this argument "simple, perhaps deceptively so,"[14] and determined that it was undermined by the structure and legislative history of the SCA.

The SCA provides, in relevant part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system 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.[15]

Several ambiguous aspects of the SCA were contested in the Microsoft case. First, the term "using the procedures described in the Federal Rules of Criminal Procedure" is imprecise. At

issue was Federal Rule 41, which governs searches and seizures. Microsoft argued that the entirety of Rule 41 was incorporated in the SCA, including the territorial limitations, which means the search would be limited to the United States. Francis found it equally conceivable that only the procedural aspects of Rule 41 apply and that the substantive rules are separate, meaning that the territorial limits do not apply.

Additionally, the SCA does not address cross-border discovery, and there is little clarity from Congress or administrative agencies on how to apply the SCA to cross-border issues. In his ruling, Francis examined the "scant"[16] history of the SCA to determine how to apply the cross-border issue and determined, based on the language of the Patriot Act, that the "location" of electronic property should be based on the location of the Internet service provider, rather than the location of any particular server.[17]

Legislative history aside, Francis found that the heart of the issue was not where the data was actually stored, but whose control it was under: "It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information."[18] As the company that controls the data, Microsoft, according to Francis, could not insulate itself from the requirements of the SCA by claiming that the data was abroad.

### Next Steps

Microsoft has vowed to fight, stating that "the District Court's decision would not represent the final step in this process."[19] The case has also taken on new significance in light of current high-profile issues surrounding personal privacy and security of information stored in the "cloud." The recent theft of photographs and data from celebrities has raised enormous privacy concerns about individual users' personal data. Businesses and private individuals use email and cloud storage services routinely, but generally are unaware of the specific location of the information being stored, as well as the effect that the storage location may have on the data's privacy.

Non-U.S. companies that rely on Microsoft or other American companies for cloud services may be particularly fearful of the potential impact of the ruling in the Microsoft matter. With such jurisdiction, the U.S. government would be able to obtain the data of these companies through their cloud services providers by means of discovery or subpoena.

The court system has been placed in the unenviable position of determining the intent of the Stored Communications Act, a law that was passed before the popularity of the Internet and does not specifically address cross-border discovery issues.

Congress has also entered the fray: On Sept. 18, 2014, U.S. Senators Orrin Hatch (R-Ut.), Chris Coons (D-Del.), and Dean Heller (R-Nev.) introduced the bipartisan Law Enforcement Access to Data Stored Abroad (LEADS) Act, which seeks to amend the ECPA (of which the SCA is a key component) so that search warrants can only be issued extraterritorially where the accountholder is a "United States person." A United States person is defined as a citizen or permanent resident of the United States, or an entity organized under U.S. laws. The LEADS Act was immediately praised by Microsoft General Counsel Brad Smith for "propos[ing] a more principled legal blueprint for balancing law enforcement needs with consumer privacy rights."[20]

### Conclusion

The court system has been placed in the unenviable position of determining the intent of the Stored Communications Act, a law that was passed before the popularity of the Internet and does not specifically address cross-border discovery issues. In his ruling on Microsoft's motion to quash its search warrant, Francis sought to balance the role of law enforcement in obtaining information with the privacy concerns that businesses and private individuals may face.

Technological progress in recent years has challenged previous notions of how the legal field should address electronic discovery. The SCA itself was developed as a response to advances of the late 20th century, and as certain portions of it become obsolete or outdated, it is imperative that technological advances be addressed. Congress has taken a step in the right direction by proposing clarity on how the ECPA may apply to data stored abroad. As cross-border electronic discovery issues become increasingly complicated, it is important that more guidance be provided by lawmakers and that companies and legal practitioners gain a better appreciation for the weighty issues at stake.

1. Available at http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm (last accessed Sept. 23, 2014).
2. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13-mj-02814, 2014 WL 1661004 (S.D.N.Y. April 25, 2014), at *2.
3. Id. at *1.
4. Apple and Cisco Systems filed a joint brief.
5. Memorandum of Law in Support of Verizon Communications' Motion to Participate as Amicus Curiae and Microsoft's Motion to Vacate Search Warrant, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13-mj-02814, ECF No. 29 (S.D.N.Y. June 10, 2014), at 1-2.
6. Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13-mj-02814, ECF No. 9 (S.D.N.Y. April 25, 2014).
7. Brad Smith, Op-Ed., "We're Fighting the Feds Over Your Email," Wall St. J., July 29, 2014, http://online.wsj.com/articles/brad-smith-were-fighting-the-feds-over-your-email-1406674616.
8. *In the Matter of a Warrant to Search*, 2014 WL 1661004 (S.D.N.Y. April 25, 2014), at *4.
9. Memorandum in Support of Microsoft's Motion to Vacate in Part an SCA Warrant Seeking Customer Information Located Outside of the United States, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13-mj-02814, ECF No. 6 (S.D.N.Y. April 25, 2014), at 6.
10. Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13-mj-02814, ECF No. 15 (S.D.N.Y. June 6, 2014), at 4.
11. Government's Memorandum of Law in Opposition, No. 13-mj-02814, ECF No. 9 (S.D.N.Y. April 25, 2014), at 16.
12. *In the Matter of a Warrant to Search*, 2014 WL 1661004 (S.D.N.Y. April 25, 2014), at *5.
13. 706 F.3d 92 (2d Cir. 2013).
14. *In the Matter of a Warrant to Search*, 2014 WL 1661004 (S.D.N.Y. April 25, 2014), at *3.
15. Id. at *4 (citing 18 U.S.C. §2703(a)).
16. Id. at *6.
17. Id. at *7.
18. Id. at *5.
19. Ellen Nakashima, "Judge Orders Microsoft to Turn Over Data Held Overseas," Wash. Post, July 31, 2014, http://www.washingtonpost.com/world/national-security/judge-orders-microsoft-to-turn-over-data-held-overseas/2014/07/31/b07c4952-18d4-11e4-9e3b-7f2f110c6265_story.html.
20. Nancy Scola, "Senate's New Overseas-Email Protection Act Gets Mixed Reviews," Wash. Post, Sept. 18, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/senates-new-overseas-email-protection-act-gets-mixed-reviews/.