New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 20
WEDNESDAY, JULY 30, 2014

INTERNATIONAL CRIMINAL LAW AND ENFORCEMENT

Expert Analysis

End Run: Using Search Warrants To Obtain Foreign Records

By **Nicholas M. De Feis**

And **Philip C. Patterson**

In a previous column, we wrote about the Securities and Exchange Commission's authority to compel a domestic corporation to produce documents in the possession of an overseas subsidiary when doing so might run afoul of foreign laws.[1] In this column, we write about a similar issue—the authority of the Department of Justice to compel a domestic corporation to produce emails stored on an overseas server.

In a recent opinion in the Southern District of New York, Magistrate Judge James Francis denied Microsoft's motion to quash a warrant seeking emails stored in an overseas data center.[2] Microsoft is challenging the judge's opinion and the parties have further briefed the issue. Oral arguments are scheduled for July 31, 2014.

If upheld, the opinion seemingly represents a substantial expansion of the Department of Justice's power to use warrants to compel production of electronic data stored overseas and an end run around Mutual Legal Assistance Treaties. A number of major technology companies have filed amicus briefs supporting Microsoft's objections to the opinion. The opinion, however, may not be the expansion of authority or invasion of privacy that Microsoft and the amicus curiae claim it is. Instead, it may simply be an acknowledgment by the court that the increasing prevalence of digital communications is breaking down the distinctions between borders and jurisdictions. In fact, the opinion may be an indication that the traditional expectations of privacy or perhaps sovereignty itself simply do not apply in our interconnected digital world.

Motion to Quash

On Dec. 4, 2013, the U.S. Attorney's Office for the Southern District of New York obtained a search warrant for information associated with an email account controlled by Microsoft. Apparently the warrant was part of a narcotics investigation. Microsoft produced certain information stored in the United States but moved to quash the warrant to the extent it sought information stored overseas.

Microsoft explained that it stores information concerning customer email accounts at data centers in the United States and abroad. This information consists of "content information," such as the subject line and text of an email, and "non-content information," such as the date and time of an email and the addresses of the sender and recipient. In 2010, Microsoft began "migrating" stored information for email accounts to the data centers located closest to the respective customers. The shorter distances mean faster transmission, and the new procedure appears totally unrelated to any desire to insulate communications from disclosure. Information stored overseas can be viewed onscreen by Microsoft employees within the United States.[3]

The account in question was registered with a country code of Ireland. Consistent with Microsoft's procedures, the information associated with the account had migrated to a data center in Dublin, Ireland, and all content information and most non-content information maintained in the United States had been

NICHOLAS M. DE FEIS *is a partner at De Feis O'Connell & Rose and a former federal prosecutor.* PHILIP C. PATTERSON *is counsel to the firm.*

deleted. In response to the warrant, Microsoft produced the non-content information for the account that was still stored in the U.S. but moved to quash the warrant to the extent it sought the content information stored in Ireland.[4]

The dispute centers on the Stored Communications Act (SCA), which was passed as part of the Electronic Communications Privacy Act of 1986.[5] The law makes it a crime to access information stored by Internet service providers (ISPs) without authorization, but permits the government to use warrants, subpoenas or court orders to compel production of such materials. In this case, the likely reason the government used a warrant rather than a subpoena is because a subpoena issued pursuant to the SCA requires notice to the customer and provides an opportunity to challenge it in advance. The SCA also requires the government to use a warrant if it seeks unopened emails that have been stored for 180 days or less (courts have held that opened emails are no longer in storage for the purposes of the SCA). But regardless of whether a warrant or subpoena is used, the SCA generally refers to the Federal Rules of Criminal Procedure for the applicable procedures and standards.

Microsoft's core argument was simple: Courts are not permitted to issue warrants for extraterritorial searches and seizures. Although subpoenas can compel production of materials outside the U.S. that are under the possession, custody or control of a party within the U.S., warrants cannot. Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, courts can only issue warrants for searches and seizures of persons or property located within their district, which limits application to persons or property within the U.S.

Microsoft thus argued that because the government sought the information stored in Dublin through a warrant, rather than a subpoena, the warrant constituted an improper extraterritorial search and seizure.[6]

The court's opinion acknowledged the government's lack of authority to execute extraterritorial warrants. The court also noted that the SCA was essentially passed to create Fourth Amendment-like privacy protections regulating access to stored electronic information. But the court found ambiguity in whether the SCA's reference to the federal rules of procedure restricted its application to those rules or whether broader authority may come from other sources. Finding ambiguity, the court considered statutory structure and legislative intent.[7]

Magistrate Judge James Francis denied Microsoft's motion to quash a warrant seeking emails stored in an overseas data center.

As for statutory construction, the court noted that although the SCA uses the term "warrant" to describe an instrument by which the government can compel production of electronic information, a warrant issued pursuant to the SCA is different than a typical warrant issued under the Federal Rules. A "warrant" issued pursuant to the SCA is not executed by having agents enter a premises and conduct a search. Instead, the warrant is served on an electronic service provider like a subpoena. The court thus concluded that an SCA warrant is a hybrid creation somewhere between a traditional warrant and subpoena.

Based on this, the court agreed with the government's argument that the structure of the SCA—which authorizes warrants executed like subpoenas—does not raise extraterritorial limitations. The court also seemingly concluded that the search in this case does not occur when Microsoft copies the materials on its Dublin server and gives them to the government, and instead only occurs when the government views the materials within the U.S. The court concluded that this is not an extraterritorial search.[8]

As for legislative history, the court described it as "scant." The court noted, however, that Section 108 of the Patriot Act amended 18 U.S.C. §2703—the section of the SCA that authorizes the government to compel production from ISPs. The amendment authorizes a court overseeing an investigation to issue a warrant directly, without the need to go through a court in the district where the ISP is located. The legislative history of the amendment explains that it was an attempt "to address the investigative delays caused by the cross-jurisdictional nature of the Internet." The Microsoft court noted that this explanation assumed that the location of the information for the purposes of the SCA was the location of the ISP, rather than any of its servers.[9]

Finally, the Microsoft court concluded that "practical considerations" weighed in favor of finding extraterritorial application of SCA warrants. The court concluded that Congress could not have intended SCA warrants to apply only to electronic data stored within the United States. The court suggested that if that were true, the only recourse for government investigations would be time-consuming applications pursuant to Mutual Legal Assistance Treaties (MLATs). The court noted that investigations could be hindered

because countries sometimes simply reject proper MLAT requests.[10] The court thus denied Microsoft's motion to quash.

Microsoft filed objections to the opinion, arguing that there is nothing ambiguous about the use in the SCA of the term "warrant." Microsoft argued that the opinion provides an end-run around limitations on extraterritorial application as well as MLATs. Microsoft accused the court of using a "mix and match" that permits the government to "exploit the power of a warrant and the sweeping geographic scope of a subpoena, without having to comply with the fundamental protections provided by either."[11]

Microsoft is receiving support in the form of amicus briefs filed by Verizon, AT&T, Apple, Cisco, software company Infor and the Electronic Frontier Foundation. These briefs raise issues inherent in virtually every request for overseas discovery—the potential for conflict where compliance with domestic law violates foreign law and the resulting need to rely on international channels such as MLATs. The briefs also argue that electronic documents exist where they are stored, and not in any place from which they can be viewed or downloaded. Microsoft and the amicus curiae also make a broader policy argument by arguing the interest in attempting to maintain individual privacy in an increasingly interconnected digital world.

Implications

The court's opinion represents a potential expansion of the government's ability to compel production of electronic materials stored overseas. Indeed, taking a step back from the technical statutory analysis, Microsoft makes a compelling point. The SCA authorizes the government to compel information using warrants, subpoenas or court orders. These are distinct procedural devices. If Congress intended to create a new hybrid SCA warrant that operates with the broad geographical scope of a subpoena, presumably it would have said so.

Yet, underlying the opinion is an acknowledgment of the realities of today's technology. Traditional search and seizure law may fit uncomfortably in a digital world. Indeed, there is something ludicrous about the notion that an email that can easily be viewed on a monitor in Manhattan actually only exists on a server in Ireland.

The Microsoft court concluded that 'practical considerations' weighed in favor of finding extraterritorial application of Stored Communications Act warrants. The court concluded that Congress could not have intended SCA warrants to apply only to electronic data stored within the United States.

Many of the issues implicated in the Microsoft case were recently considered by the Supreme Court. In *Riley v. California*, decided only a month ago, the Supreme Court ruled 9-0 that a cell phone seized during a lawful arrest could not be searched by the police without a warrant.[12] Underlying the court's opinion was the interest in attempting to maintain individual privacy in the digital world. A primary factor in the court's decision was the recognition that cell phones today can contain documentation concerning every aspect of a person's life—an amount of information that people previously did not (and could not) carry around in their pockets.

Moreover—and perhaps significant for the Microsoft case—the court noted that information accessible on a cell phone may actually be stored elsewhere. Indeed, the government in *Riley* conceded that existing exceptions to the Fourth Amendment warrant requirement could not cover such information, and new exceptions proposed by the government for warrantless cell phone searches were rejected by the court.

Like *Riley*, the Microsoft case reflects an attempt to reconcile existing legal precedents with rapidly evolving technologies. The Microsoft case presents a closer call than *Riley*, and whatever the result will likely be appealed even beyond the district court level. What is clear is that no one is trying to hide anything here. Instead, the parties are trying to interpret a law that Congress has left frustratingly unclear and then determine whether it comports with our Constitution. Until the courts resolve this, attorneys should advise their clients to assume that anything they put into an email anywhere in the world could someday be discoverable in any country in the world.

1. Nicholas M. De Feis and Philip C. Patterson, "In Seeking Documents Abroad, Does the SEC's Reach Exceed Its Grasp?" NYLJ, April 24, 2014, available at http://www.newyorklawjournal.com/id=1202597179910?.

2. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13 Mag. 2814, 2014 U.S. Dist. Lexis 59296 (SDNY April 25, 2014) (hereinafter "*In re Microsoft Warrant*").

3. *In re Microsoft Warrant*, 2014 U.S. Dist Lexis 59296 at *2-*5.

4. Id.

5. 18 U.S.C. §§2701-2712.

6. See Memorandum in Support of Microsoft's Motion to Vacate in Part, 13 Mag. 2814, ECF Docket No. 6 at 1, 5-9.

7. *In re Microsoft Warrant*, 2014 U.S. Dist Lexis 59296 at *11-*14.

8. See id. at *15-*17.

9. *In re Microsoft Warrant*, 2014 U.S. Dist Lexis 59296 at *21-*22.

10. Id. at *23-*25.

11. Microsoft Objections to the Magistrate's Order, 13 Mag. 2814, ECF Docket No.15 at 2.

12. 189 L. Ed. 2d 430; 2014 U.S. LEXIS 4497 (June 25, 2014).