New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 72
MONDAY, APRIL 17, 2017

INTERNATIONAL CRIMINAL LAW AND ENFORCEMENT

Expert Analysis

Will Tech Firms Be Compelled To Produce Overseas Emails?

By **Nicholas M. De Feis**

And **Philip C. Patterson**

An issue with significant potential to affect the relationships between U.S. law enforcement and technology companies and their customers remains unresolved and could be destined either for the U.S. Supreme Court or a legislative fix. Back in 2014, a dispute emerged in the Southern District of New York over whether the U.S. government can compel Microsoft to produce email data in the United States that is stored on a server in Ireland. The issue turns on the government's authority to seek warrants under the Stored Communications Act (SCA). The District Court denied Microsoft's motion to quash the warrant, but last year the Second Circuit disagreed and ordered that the warrant be quashed.

The issue has been hotly contested, with amicus briefs filed by multinational technology companies such as AT&T, Apple and Verizon, advocacy groups such as the ACLU, and even the Government of Ireland. The question appears to be settled in the Second Circuit, and only days ago the New York Court of Appeals cited the Second Circuit's reasoning in an opinion concerning the interplay between the SCA and New York State law. But courts in other circuits have recently declined to follow the Second Circuit, indicating that the issue is unresolved.

Background

In December 2013, the Southern District U.S. Attorney's Office obtained a search warrant concerning a Microsoft web-based email account.[1] The government sought the information in a narcotics investigation. Microsoft was served with the warrant at its headquarters in Washington. As is increasingly common, however, Microsoft had processes in place whereby email data migrated between multiple servers to optimize efficiency. The account in question had been opened with a country code of Ireland, so data from the account automatically migrated to a server in Dublin. The data stored in the United States was deleted, except for basic account information. Yet, the data stored in Dublin—which included the content of the emails—could be collected and viewed by certain Microsoft employees in the United States.

An issue with significant potential to affect the relationships between U.S. law enforcement and technology companies and their customers remains unresolved and could be destined either for the U.S. Supreme Court or a legislative fix.

The government sought the warrant pursuant to the SCA. The SCA gives Fourth Amendment-like protections to information stored with email service providers, but

NICHOLAS M. DE FEIS *is a partner and* PHILIP C. PATTERSON *is counsel at De Feis O'Connell & Rose, where they practice white-collar criminal defense and international investigations. Mr. De Feis is a former federal prosecutor.*

authorizes subpoenas, warrants or court orders to compel production. The government chose to seek a warrant either because the SCA requires warrants for recently stored emails or because SCA subpoenas for the content of emails require that notice be provided to the accountholder.

Microsoft produced the U.S. data but moved to quash the warrant as to the overseas data. Microsoft's core argument was simple: Courts can only issue warrants for searches and seizures of persons or property located within the United States. Microsoft argued that compelling production of data stored in Ireland amounts to an improper extraterritorial warrant.

In an April 2014 opinion, Magistrate Judge Francis found ambiguity in the SCA and considered statutory structure and legislative intent. The court noted that SCA warrants are served on service providers, who must then produce responsive materials. The court reasoned that SCA warrants thus are unlike traditional warrants, which are served by agents before they themselves perform a physical search. Instead, they are akin to a traditional subpoena, which is served on a party who must then produce responsive materials in their possession, custody or control regardless of where it is located in the world. The court added that because the email data would actually be viewed in the United States, there would be no extraterritorial search.

The court noted that although there is little relevant legislative history, Congress included an amendment to the SCA in the Patriot Act to streamline the warrant procedure. The amendment authorizes a court overseeing an investigation to issue a warrant directly, without having to go through a district court where the service provider is located. The court observed that this change assumed that the location of the information for the purposes of the SCA was the location of the service provider itself, rather than its servers.

Finally, the court concluded that "practical considerations" weighed in favor of compelling production. Congress could not have intended SCA warrants to apply only to data stored within the United States. Otherwise, the court reasoned, the only recourse for the government would be time-consuming and unreliable applications pursuant to Mutual Legal Assistance Treaties.

> Many of these opinions rightly call for a legislative solution. The legislature should take up these issues, rather than leave it to the courts to try to determine how 30-year-old statutory language applies to technology that changes almost daily.

The court denied Microsoft's motion to quash. Microsoft appealed to Chief Judge Loretta Preska. She reviewed the issue de novo and, after holding a hearing, affirmed Judge Francis' opinion. Microsoft appealed to the Second Circuit.

The Second Circuit Opinions

In July 2016, the Second Circuit reversed the District Court and ordered that the warrant be quashed as to the overseas data.[2] The Second Circuit began its analysis by noting that the situation could not even have been contemplated when the SCA was drafted 30 years ago. The court also observed that neither party disputed that the materials in question were located in Ireland, and that Microsoft would have to retrieve them to produce them in the United States. In addition, the record did not indicate the citizenship of the individual who opened the account.

The Second Circuit's analysis relied on the Supreme Court's opinion in *Morrison v. National Australian Bank* for the principle that there is a strong presumption against extraterritorial application of U.S. laws.[3] The court noted that if Congress intends a law to apply outside the United States, this intent is made clear through an "affirmative indication." The court found no such indication in the SCA. The court added that the term "warrant" has long been understood to refer to domestic searches. The court also disagreed that the Patriot Act amendment authorizing nationwide service of warrants meant the SCA could reach across borders. The court further held that serving SCA warrants like subpoenas was not so determinative, given that agents executing traditional warrants sometimes compel persons to assist in their searches.

Having found that Congress did not intend the SCA to apply extraterritorially, the court next considered the second part of the *Morrison* analysis—looking to the "focus" of the statute to determine whether it applies domestically. The court held

that the language of the SCA and its legislative history make clear that the focus is on protecting privacy. The court then disagreed with the lower court that the search would occur in the United States after the data is retrieved, and concluded that the actual seizure of the data occurs in Ireland. The Second Circuit held that this would amount to extraterritorial application.

The government subsequently requested a rehearing en banc, which was denied in January 2017 when the court split 4-4 with three judges recused. The Second Circuit's opinions include a concurrence and dissents, each calling for Congress to take up the issue. Concerns cited by the judges include reconciling the government's interest in law enforcement with privacy rights, and updating the SCA to meet the realities of modern technology.

Recent Decisions

On Feb. 3, 2017, the Eastern District of Pennsylvania issued an opinion regarding an SCA warrant served on Google.[4] The accountholders in question were located in the United States, but Google, like Microsoft, employs processes that automatically break up and migrate data for efficiency. Google argued that the data can even move between the time the warrant is sought and served. Google produced the data it could verify was located in the United States but, based on the *Microsoft* opinion, declined to produce overseas data. The government moved to compel.

The *Google* court agreed with the Second Circuit that the focus is on privacy, but adopted Judge Francis' and the Second Circuit dissenting opinion's reasoning that the invasion of privacy would occur in the United States after Google employees retrieve the data from overseas. The court added that retrieval also would not constitute a seizure because the data would still be accessible to the customer. The court granted the government's motion to compel. Google filed objections, and a district judge has been assigned to hear arguments by the parties and many amici curiae from the *Microsoft* case.

On Feb. 21, 2017, the Eastern District of Wisconsin issued an opinion in a similar matter involving Yahoo and Google accounts.[5] The court agreed with the Second Circuit dissent and quoted its reasoning that "if the recipient can access a thing here, then it can be delivered here." The court also adopted the reasoning that an SCA warrant operates like a subpoena. Google is challenging the Magistrate Judge's opinion, but the docket concerning the Yahoo account is sealed so its status is unclear.

Finally, on April 4, 2017 the New York Court of Appeals issued an opinion denying Facebook standing to challenge an SCA warrant issued to the Manhattan District Attorney's Office.[6] Under New York law, an opinion denying a motion to quash a subpoena can be appealed, while an opinion denying a motion to quash a warrant cannot. The court conducted an analysis under New York law, but also cited the Second Circuit's reasoning in concluding that an SCA warrant is a true warrant—and not a subpoena. Facebook thus did not have standing under New York law to challenge SCA warrants seeking the content of customer accounts, but a lengthy dissent disagreed and argued that SCA warrants are more akin to subpoenas.

Conclusion

The number and prominence of amici curiae in these cases makes clear the significance of these issues. Each of the aforementioned opinions recognizes that the challenge is to properly balance the interests in privacy, law enforcement and even international comity. Different outcomes in different courts also raise the possibility of district-shopping.

Many of these opinions rightly call for a legislative solution. The legislature should take up these issues, rather than leave it to the courts to try to determine how 30-year-old statutory language applies to technology that changes almost daily.

1. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft*, No. 13 Mag. 2814, 2014 U.S. Dist. Lexis 59296 (S.D.N.Y. April 25, 2014).

2. *Microsoft v. United States*, 829 F.3d 197 (2016).

3. 561 U.S. 247 (2010).

4. *In re Search Warrant No. 16-960-M-01*, 2017 U.S. Dist. LEXIS 15232 (E.D. Pa. Feb. 3, 2017).

5. *In re Info. Associated with Yahoo Address*, 2017 U.S. Dist. LEXIS 24591 (E.D. WI Feb. 21, 2017).

6. *Matter of 381 Warrants Directed to Facebook*, 2017 NY Slip Op 02586 (N.Y. April 4, 2017).

Reprinted with permission from the April 17, 2017 edition of the NEW YORK LAW JOURNAL © 2017 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-04-17-21