Morgan Lewis

LAWFLASH

DECISION HOLDS THAT SEARCH WARRANT CANNOT COMPEL DATA STORED OVERSEAS

July 15, 2016

AUTHORS AND CONTACTS

Mark L. Krotoski, Ellie F. Chapman

The landmark ruling is the first by a federal court of appeals to address the extraterritoriality of the Stored Communications Act.

Microsoft and other US-based internet service providers won a major victory on July 14 at the US Court of Appeals for the Second Circuit, which held that the company is not required to comply with a federal search warrant for customer emails stored on a server in Dublin, Ireland.[1] The ruling is the first by a federal court of appeals to address the extraterritoriality of the Stored Communications Act (SCA) often used in government investigations to obtain data.[2] Whether other courts will follow this groundbreaking ruling remains to be seen.

CASE BACKGROUND

The case involved a search warrant issued by a federal judge in New York for the email content and records of a suspect in a drug trafficking investigation. The search warrant was issued under the SCA, a statute first enacted in 1986 and amended by Congress over the years. Upon a proper showing, the government uses the SCA to compel disclosure of information from network service providers, including the content of electronic communications, transactional records and account logging information, and customer account information.[3]

The wrinkle in the case was that some of the requested data was stored in Microsoft computers in Ireland. In response to the search warrant, Microsoft provided noncontent data on the requested email account that was stored in the United States but filed a motion to quash the search warrant for customer content data stored in Ireland, arguing that the government lacked authority to compel the production of data stored outside the United States. The SCA is silent on the statute's reach outside the United States, including under the warrant provision.

On April 25, 2014, a federal magistrate judge ruled that Microsoft must produce the emails stored on the

Ireland-based Microsoft computers.[4] In doing so, the magistrate judge adopted the government's view that an SCA warrant is more akin to a subpoena than a search warrant and that a properly served subpoena would compel production of any material, including customer content, so long as the material is stored at premises "owned, maintained, controlled, or operated by Microsoft Corporation." The fact that those premises were located abroad was, in the magistrate judge's view, of no consequence.

On July 31, 2014, the district judge overseeing the matter upheld the search warrant but stayed the ruling pending appeal. At the hearing, the district judge concluded that "the structure, language, legislative history, Congressional knowledge of precedent, . . . all lead to the conclusion that Congress intended in this statute for ISPs to produce information under their control, albeit stored abroad, to law enforcement in the United States."[5] Microsoft appealed the ruling to the Second Circuit. The case was argued on September 9, 2015, and many have been awaiting the ruling on the novel issues presented in the case.

THE SECOND CIRCUIT RULING

On July 14, 2016, the Second Circuit overturned the lower court's ruling, holding that the SCA's Warrant Provisions do not give investigators the ability to force Microsoft to produce data stored on overseas servers.[6] In its ruling, the Second Circuit focused on the presumption against extraterritorial application of US statutes—meaning that congressional legislation is presumed to apply only within the territorial jurisdiction of the United States, unless a contrary intent clearly applies.[7]

With this principle in mind, the Second Circuit analyzed the SCA's warrant provision to determine whether Congress contemplated extraterritorial application of the statute. The court "disposed of this question with relative ease," given that the government conceded at oral argument that the warrant provision of the SCA did not contemplate or permit extraterritorial application. The Second Circuit then "confirm[ed] the soundness" of the government's concession through an analysis of the statute's plain meaning. The court found it significant that no provision in the SCA mentioned any extraterritorial application or even alluded to any such application. The court also found it instructive that the SCA used the term "warrant," a centuries old legal term moored in privacy concepts applied within the territory of the United States. In doing so, the circuit rejected the lower court's finding that an SCA warrant more closely resembles a subpoena than a warrant.

The court then went on to determine the SCA's focus. Through an analysis of the statute's various provisions and legislative history, the court concluded that the SCA's main focus was to protect users' privacy interests in stored communications. Having determined that the SCA did not contemplate extraterritorial application and that the SCA focused on user privacy, the court held that the execution of the warrant in this instance would constitute an unlawful extraterritorial application of the SCA. The district court "lacked authority to enforce" the search warrant. In reversing, the case was remanded "with instructions to the District Court to quash the Warrant insofar as it directs Microsoft to collect, import, and produce to the government customer content stored outside the United States."

CONCURRENCE

In a concurring opinion, Second Circuit Judge Gerard E. Lynch agreed with the holding of the majority opinion that the SCA should not be construed to require Microsoft to turn over email content stored on Ireland servers but wrote separately to clarify his view that the dispute in this case was not about privacy,

but rather about the international reach of US law.

His concurrence noted that—contrary to the majority opinion, which emphasized how this case posed a government threat to individual privacy—the case involved the issuance of a search warrant based on probable cause. In other words, the government had already complied with the most restrictive privacy-protecting requirements of the SCA as well as the highest level of protection ordinarily required by the Fourth Amendment. In light of this fact, Judge Lynch rephrased the issue in the case as "whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country." He noted, moreover, that the opinion represented a win for consumer privacy "as against the government." But that consumer privacy remains protected against Microsoft only to the extent defined by a consumer's adhesion contract with the company.

Critically, Judge Lynch emphasized that questions about the international reach of US law, like the questions presented in this case, are "entirely left to Congress." In his view, the primary reason for Microsoft's victory was the lack of evidence that Congress had even considered the important policy issues at stake in this case. His concurrence emphasized, above all else, a great need for congressional action to revise a "badly outdated statute."

INITIAL RAMIFICATIONS AND OBSERVATIONS

Many have been waiting for this ruling since the case was argued 10 months ago. Some initial observations follow.

Limited Initial Precedent

Presently, the ruling only applies to federal courts in the Second Circuit, which includes Connecticut, New York, and Vermont. Federal courts outside the Second Circuit are not bound by the new ruling and may reach other conclusions. In fact, in the past, the federal courts have divided on other aspects of the SCA.

Supreme Court Review

Ultimately, the US Supreme Court may determine the SCA's reach. Normally, the Supreme Court waits to exercise its discretion to hear a case until the issue has been considered by other courts. It also remains to be seen whether the government may seek Supreme Court review in the *Microsoft* case.

Will Congress Update the SCA?

Whether Congress will intervene remains a looming question, particularly in light of Judge Lynch's concurrence. For several years, legislation has been introduced to update the SCA based on contemporary practices. Each time, the legislation has stalled.

The opinion, of course, turned on the Second Circuit's interpretation of the SCA—a 30-year-old statute passed before the widespread use of email, instant messages, and storage of data on networks of servers located around the world. Today, information is increasingly being housed in massive international data centers, a situation that the SCA could hardly have anticipated when it was written three years before the invention of the World Wide Web. Ultimately, Congress may decide how to strike the privacy balance and what standards and scope will apply to government demands for data.

Impact on Recent EU Data Transfer Issues

For now, the court's ruling also avoids a major conflict between EU and Irish laws that protect personal data located in Ireland from being delivered to US law enforcement through a warrant from the United States. The US government's ability to compel the production of personal data located abroad has been a significant policy issue concerning the establishment of an EU-US Privacy Shield.[8] The court decision also avoids a conflict with the new European General Data Protection Regulation (GDPR) and the *Schrems* decision of the European Court of Justice of last October.[9]

Scope of Government Authority to Compel Data Production

The ruling reflects another round as part of a broader fight between Silicon Valley (and other technology companies) and Washington over how much authority the government has to force technology companies to provide data in investigations.

On the other hand, the government, in some circumstances, may now be faced with the additional hurdle of requesting evidence through foreign governments—through a Mutual Legal Assistance Treaty request—a process that can be time-consuming and onerous.[10]

Fact-Specific Inquiry

The question on the scope of the government's authority will continue to turn on the particular facts of the case. The manner in which the data is obtained and stored abroad may be relevant.

In the *Microsoft* case, the data was automatically stored in Ireland based on the user's country code. Upon the transfer of the data to Ireland, "all content and non-content information associated with the account in the United States" was deleted from US-based servers. In other cases, the facts of storage may vary.

In contrast, if the customer emails had existed somewhere in the United States at the time of the proceedings, there would have been no need for the Second Circuit to consider the presumption against extraterritoriality at all, and the government would have been able to likely obtain the suspect's emails.

The question of where data is actually located at any given time becomes particularly challenging when one considers the various and complex methods of data storage. For instance, "load balancing," a method of data storage used by many companies, distributes workloads across multiple computing resources to optimize resource use and avoid overload of any single resource. In other words, data stored by "load balancing" will be in one location in one minute—and another location the next. The inquiry becomes more challenging still when one considers that each individual company will likely have different practices regarding how it stores and accesses data.

CONCLUSION

The landmark Second Circuit ruling sheds light on an important issue confronting many companies that store some data outside the United States. Whether other courts will follow this precedent or consider other legal standards (like the two lower court judges did before the Second Circuit opinion) remains to be seen. Although the new ruling provides useful guidance on this issue, the facts of any data transfers, storage, and access will need to be considered on a case-by-case basis.

CONTACTS

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis lawyers:

Philadelphia
Tess Blair
Gregory T. Parks

London
Pulina Whitaker

New York
Gary Adler
David I. Miller

San Francisco
W. Reece Hirsch

Silicon Valley
Mark L. Krotoski

Washington, DC
Eric W. Sitarchuk
Dr. Axel Spies
Hill B. Wellford

---

[1] *Microsoft Corporation v. United States of America*, No. 14-2985 (2d Cir. July 14, 2016), http://www.ca2.uscourts.gov/decisions/isysquery/79f10115-e24e-49b3-b72b-1df1e7e97911/4/doc/14-2985_complete_opn.pdf.

[2] Stored Communications Act, 18 U.S.C. §§ 2701 *et seq*.

[3] 18 U.S.C. §§ 2703(a)-(c).

[4] *In The Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014).

[5] *In The Matter Of A Warrant To Search A Certain E-Mail Account Controlled And Maintained By Microsoft Corporation*, No. 13 MJ 2814, Hearing Transcript, at 69 (July 31, 2014).

[6] *Microsoft Corporation v. United States of America*, No. 14-2985 (2d Cir. July 14, 2016), http://www.ca2.uscourts.gov/decisions/isysquery/79f10115-e24e-49b3-b72b-1df1e7e97911/4/doc/14-2985_complete_opn.pdf.

[7] *See, e.g.*, *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010); *see also RJR Nabisco, Inc. v. European Cmty.*, No. 15-138, 579 U.S. __, 2016 WL 3369423 (June 20, 2016), https://www.supremecourt.gov/opinions/15pdf/15-138_5866.pdf.

[8] Authorities and parties in Europe have claimed that the US authorities should follow the procedures under the so-called Hague Convention and Mutual Legal Assistance Treaties with Ireland. *See, e.g.*,

LawFlash, Article 29 Working Party Expresses Concerns About EU-US Privacy Shield (April 14, 2016), https://www.morganlewis.com/pubs/article-29-working-party-expresses-concerns-about-eu-us-privacy-shield#sthash.2RVULlrP.dpuf.

[9] In particular, Art. 48 GDPR, see LawFlash https://www.morganlewis.com/pubs/ecj-rules-eu-us-safe-harbor-programme-is-invalid on the ECJ's Schrems decision.

[10] In fact, an MLAT between the United States and member states of the European Union, including Ireland, was adopted in 2003. *See* Agreement on Mutual Legal Assistance Between the European Union and the United States of America, June 25, 2003, T.I.A.S. No. 10-201.1.