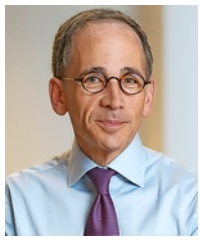
Bloomberg BNA

Privacy and Security Law Report®

Data Protection

The Second Circuit's challenge in considering the validity of a U.S. Stored Communications Act warrant to Microsoft for e-mails located on servers in Ireland involves interpreting the SCA, which was enacted nearly three decades ago, long before today's Internet, cloud storage and huge amounts of data stored around the world, the author writes.

United States v. Microsoft: 'Global Chaos,' Outdated Legislation And a Judge's Plea to Congress



By Craig A. Newman

Craig A. Newman is a litigation partner at Patterson Belknap Webb & Tyler LLP in New York and chair of the firm's Data Security and Privacy Practice. He is recognized as a leading authority on cybersecurity issues and advises global institutions, Fortune 500 companies, investment funds, their boards and leadership teams on data security practices, policies and governance issues including investigations, regulatory matters and litigation.

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

When the U.S. Court of Appeals for the Second Circuit heard oral argument in September in a case concerning Microsoft Corp.'s refusal to comply with a government search warrant and handover the contents of customer e-mails stored on a server in Ireland, Judge Gerald E. Lynch ended the almost 90-minute argument with an unusual plea: ''I do think the one thing that probably everyone agrees on is that, as so often, it would be helpful if Congress would engage in that kind of nuanced regulation, and we'll all be holding our breaths for when they do.''[1]

Judge Lynch's closing observation illustrates the challenge facing the Second Circuit in interpreting the Stored Communications Act (SCA), a statute enacted into law nearly three decades ago, long before today's Internet, long before cloud storage and long before huge amounts of data was stored in servers around the world.

And, as more and more digital information is stockpiled, it will be increasingly critical for global businesses to understand the rules of the road and precisely when, under what circumstances, and how governments in the U.S. and abroad can lawfully access that data, wherever collected and stored. As the court itself acknowledged during oral argument, the ''implications. . . [of its ruling] are obviously broad.''[2] That's es-

[1] Hearing Transcript, *United States v. Microsoft*, No. 14-2985-CV, 9/9/15, at p. 99 (Hearing Transcript) (14 PVLR 1678, 9/14/15)

[2] *Id.* at p. 74.

 ISSN 1538-3423

pecially so as our digital universe expands. By one estimate, the digital universe – meaning the data we create and copy – will reach 44 zettabytes or 44 trillion gigabytes by 2020. That means within the next five years there will be as many digital bites as stars in the universe.[3]

The three-judge panel included Judge Lynch,[4] a former Columbia Law School professor and U.S. District Judge; Susan L. Carney, former Deputy General Counsel of Yale University; and Victor A. Bolden, a U.S. District Judge for the District of Connecticut, who was sitting by designation.

The Facts: Microsoft, DOJ and the SCA

At issue on the appeal is whether a U.S. warrant issued under the SCA can reach data stored on a server in Europe. Microsoft has fought the case for the past two years, starting in December 2013 when, in connection with a drug-trafficking investigation, U.S. law enforcement officials served a warrant on Microsoft at its headquarters in Redmond, Wash.. The warrant sought e-mail traffic including e-mail content associated with an unnamed user's msn.com account. It's not known whether the account belongs to a U.S. or European citizen.[5]

When Microsoft received the SCA warrant, its Global Criminal Compliance team determined that it would comply 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.[6]

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[.][7]

Throughout the case, Microsoft has read the statute as prohibiting the application of an SCA warrant beyond U.S. soil. Its position is based, in part, on the statutory language that the 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 . . . .''[8]

But Magistrate Judge James Francis disagreed and denied Microsoft's motion to vacate the warrant in April 2014 (13 PVLR 796, 5/5/14). In his ruling, Magistrate Francis concluded that the SCA itself was ambiguous and looked to its legislative history. In so doing, he concluded that an SCA warrant ''is a hybrid: part search warrant and part subpoena.''[9] An SCA warrant is obtained by demonstrating probable cause to a magistrate. But, once the SCA warrant is issued, it functions more like a subpoena because it is merely served on an Internet Service Provider (ISP)—with the onus shifting to the recipient to look for responsive materials and produce them. The 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. With a traditional subpoena, the physical location of the documents sought isn't relevant but what matters is whether the documents sought are within the possession, custody or control of the recipient.[10]

Magistrate Francis also concluded that, while the legislative history wasn't a model of clarity, it suggested that the SCA warrant did not call for extra-territorial application. He cited a House Report accompanying a 2001 amendment to the SCA that looked to the operation of Rule 41. The report compared ''where the property is located'' with the location of the ISP, not the location of any server.''[11]

Finally, Magistrate Francis looked to the practical implications of not enforcing the SCA warrant. For technical and customer service reasons, data is stored on servers located close to a user's residence. Because an ISP isn't required to verify the residence of a user, wrongdoers could provide false information to an ISP, have their e-mail data reside abroad and escape the reach of U.S. law enforcement. Further, if the SCA warrant wasn't enforced, the government would be required to use the Mutual Legal Assistance Treaty (MLAT) process, which is sometimes considered unwieldly. Magistrate Francis also noted that the U.S. has MLAT treaties with only 60 countries, suggesting that some information would be beyond the reach of U.S. law enforcement. An MLAT is an agreement between the U.S. and a foreign government to facilitate cooperation between law enforcement authorities for search warrants and court orders.[12]

In July 2014, Judge Loretta A. Preska of the U.S. District Court for the Southern District of New York affirmed Magistrate Francis's order from the bench, hold-

---

[3] John Gantz and David Reinsel, *The Digital Universe in 2020* (December 2012).

[4] Judge Lynch was the author of a 97-page decision handed down by the Second Circuit in May 2015 which ruled the once-secret National Security Agency (NSA) program that collected bulk phone records of U.S. citizens was illegal under a provision of the USA PATRIOT Act (14 PVLR 822, 5/11/15). The ruling was the first time a Federal appellate court had reviewed the NSA phone records program. Prior to Judge Lynch's ruling, the data collection was approved by judges serving on the Foreign Intelligence Surveillance Court, or FISA court, a secret court that oversees U.S. national security matters.

[5] *In re Warrant*, 15 F. Supp. 3d 466, (No. 13-MJ-2814) , ECF No. 80.

[6] *Id.* at 467-68.

[7] 18 U.S.C. § 2703.

[8] *Id.* at 470 (quoting 18 U.S.C. § 2703(a)(2012). *See also* Hearing Transcript at p. 17.

[9] *Id.* at 471-72.

[10] *Id.*

[11] *Id.* at 473-74 (quoting H.R. Rep. No. 99-647, at 32-33 (1986)). *See also* Orin Kerr, *What Legal Protections Apply to e-mail Stored Outside the U.S.?*, The Washington Post: Volokh Conspiracy (July 7, 2014).

[12] *In re Warrant*, 15 F. Supp. 3d at 474-77.

  PVLR ISSN 1538-3423

ing that the key issue was one of control over the user's information and not its physical location.[13]

On appeal before the Second Circuit, Microsoft's argument was straightforward: the SCA warrant requires an extra-territorial search because the information sought resides on a data server outside U.S. borders. Because there is a presumption against extra-territoriality in U.S. law coupled with the fact that the SCA does not provide for extra-territorial reach, a warrant issued under that statute cannot reach data stored outside the U.S.[14] Microsoft also argued that the proper method of seeking such material was through an MLAT. In fact, there is an MLAT in place between the U.S. and Ireland. In an amicus filing, the Government of Ireland noted that it ''would be pleased to consider, as expeditiously as possible, a request under the treaty, should one be made.''[15]

The government disputed that the SCA warrant implicates the presumption against extraterritoriality, arguing that Microsoft is a U.S. corporation, had access in the U.S. to the server in Ireland, and was therefore required to comply with the warrant.[16] Further, the government argued that, as the custodian of Microsoft's corporate and business records, the user's e-mail was a Microsoft ''business record'' and therefore subject to disclosure.[17] Microsoft took issue with the government's characterization of the e-mail as a business record, arguing that they were personal documents belonging to the account holder and not the company. During argument, Microsoft's lawyer told the court that ''[t]his notion of the government's that private e-mails are Microsoft's business records is very scary.''[18]

The back-and-forth during oral argument focused on three key issues:

Textual Interpretation of the Stored Communications Act: Extraterritoriality, Disclosure or Storage?

Judges Lynch and Carney pressed counsel on both sides for textual indications in the SCA that speak to extraterritoriality.[19] Microsoft's position was that because neither the text of the SCA, nor any expression of Congressional intent suggested otherwise, the presumption against extraterritorial application of U.S. law applied with full force. Under the circumstances, Microsoft argued that the U.S. should stick to the traditional MLAT process – especially since such a treaty was already in place with Ireland – to seek the e-mail traffic.[20]

The government's argument was based on the proposition that, so long as a U.S. company maintains care, custody or control of information called for by a court order, the physical location of that information is not relevant: ''[T]he SCA is all about disclosure, not storage,'' argued the government's lawyer.[21]

International Relations and Foreign Policy Implications

The undercurrent of several questions from Judges Lynch and Carney focused on the MLAT process itself and the fact that such a mechanism between the U.S. and Ireland did in fact exist but wasn't used in this case. Indeed, in an amicus brief, the Irish government noted that it stood ready to promptly facilitate the MLAT process.[22]

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.[23]

Microsoft urged the court to interpret the SCA in a way that ''creates the least international discord.''

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.''[24]

Judge Lynch also pressed on the question of whether production of the e-mail would violate either Irish or European Union data privacy protections. In responding, Microsoft pointed to excerpts from two amicus briefs which indicated that U.S. and EU privacy protections were distinct in this respect and that the e-mail should only be produced through the MLAT process or by order of the Irish courts.[25]

Judge Lynch raised the broader issue of whether the political or international implications requiring production of material stored abroad was a question more appropriately addressed by other branches of government. ''We don't do foreign relations,'' he said, suggesting that if a law as enacted by Congress and implemented by the Executive branch stirs up international discord, that's not a question for the courts. Said Lynch, ''If Congress passes a law and the executive wields it like a blunderbuss in such a way as to cause international tensions, that's for them to worry about.''[26]

[13] Brief of Appellant Microsoft Corporation at p. 14 (Appellant's Brief) (13 PVLR 1416, 8/11/14).
[14] Appellant's Brief at pp. 18-33; Hearing Transcript at pp. 34-35; 42-44.
[15] Brief of Amicus Curiae Ireland at p. 4.
[16] Brief of the United States of America at pp. 36-44.
[17] *Id.* *See also* Hearing Transcript at p.81.
[18] *Id.* at pp. 24-27; p. 98.
[19] *Id.* at pp. 6-8; 14-15; 27-33; 69-70.
[20] *Id.* at
[21] *Id.* at 55-56; 71;
[22] *Id.*
[23] *Id.* at pp. 32-33; 39
[24] *Id.* at 56-57.
[25] Id. at pp. 91-95. *See also* p. 57-58 for the government's rebuttal to the point that U.S. and Irish data privacy laws conflict.
[26] *Id.* at pp. 13-14.

The ''Plea'' for Congressional Action

Not surprisingly, the parties had different views on the state of the SCA in a digital era. The government argued that, although enacted decades ago, the SCA remained intact which was the best evidence that Congress intended it to apply regardless of advances in technology. Microsoft responded by noting that the statute was arcane and clearly not meant to apply in a rapidly changing technology environment in which the very materials sought weren't even in existence when the SCA was put into law.[27]

Microsoft has called for Congress to pass the Law Enforcement Access to Data Stored Abroad (LEADS) Act, (S. 512) which as currently drafted, has both domestic and international aspects. In the U.S., similar to the SCA, LEADS would establish a warrant requirement before technology firms hand over stored communications. But U.S. law enforcement would unilaterally have the ability to obtain e-mail content located outside of the U.S. when the content belongs to an American citizen. Not so for non-U.S. residents. Under those circumstances, the U.S. would go through the international MLAT mechanism. It also calls for the Justice Department to make changes to the existing MLAT process including the creation of an online tracking systems for requests and publishing yearly statistics about the volume of MLAT requests.[28]

Second Circuit's Decision: A Pit Stop to Congress or the Supreme Court?

It's unlikely that the Second Circuit's ruling—regardless of how decided—will be the last word. With several proposals pending in Washington including the LEADS Act, Congress could step in and address the issue. Perhaps more likely is an appeal to the U.S. Supreme Court. Either way, as our digital universe expands, either a legislative or judicial outcome will have broad implications for businesses that store digital data globally.

---

[27] Id. at pp. 72-73.

[28] *Id.* at pp. 33-34; S. 2871 – Law Enforcement Access to Data Stored Abroad Act (2013-14) (https://www.congress.gov/bill/113th-congress/senate-bill/2871); *See also Should governments be able to look at your data when it is stored abroad*, The Economist (Sept. 8, 2015) (http://www.economist.com/news/business-and-finance/21663902-test-case-set-determine-whether-fbi-can-access-microsofts-foreign-data-should); Wayne Rash, *Senate Holds Hearings on Updated ECPA Data Privacy, Storage Rules*, eWeek (Sept. 9, 2015) (http://www.eweek.com/storage/senate-holds-hearings-on-updated-ecpa-data-privacy-storage-rules.html); Patrick Maines, *The LEADS Act and cloud computing*, The Hill, (Mar. 30, 2015) (http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing).

  PVLR ISSN 1538-3423