In the Matter of a WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION.

No. 13 Mag. 2814.

United States District Court, S.D. New York.

Signed April 25, 2014.

Justin A. Anderson, Lorin L. Reisner, Serrin Andrew Turner, U.S. Attorney's Office, New York, NY, for Plaintiff.

467*467 *MEMORANDUM AND ORDER*

JAMES C. FRANCIS IV, United States Magistrate Judge.

"The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign." David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace,* 48 Stan. L.Rev. 1367, 1375 (1996). In this case I must consider the circumstances under which law enforcement agents in the United States may obtain digital information from abroad. Microsoft Corporation ("Microsoft") moves to quash a search warrant to the extent that it directs Microsoft to produce the contents of one of its customer's e-mails where that information is stored on a server located in Dublin, Ireland. Microsoft contends that courts in the United States are not authorized to issue warrants for extraterritorial search and seizure, and that this is such a warrant. For the reasons that follow, Microsoft's motion is denied.

Background

Microsoft has long owned and operated a web-based e-mail service that has existed at various times under different internet domain names, including Hotmail.com, MSN.com, and Outlook.com. (Declaration of A.B. dated Dec. 17, 2013 ("A.B. Decl."), 3).[1] Users of a Microsoft e-mail account can, with a user name and a password, send and receive email messages as well as store messages in personalized folders. (A.B. Decl., 3). E-mail message data include both content information (the message and subject line) and non-content information (such as the sender address, the recipient address, and the date and time of transmission). (A.B. Decl., 4).

Microsoft stores e-mail messages sent and received by its users in its datacenters. Those datacenters exist at various locations both in the United States and abroad, and where a particular user's information is stored depends in part on a phenomenon known as "network latency"; because the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter. (A.B. Decl., 6). Accordingly, based on the "country code" that the customer enters at registration, Microsoft may migrate the account to the datacenter in Dublin. (A.B. Decl., 7). When this is done, all content and most noncontent information associated with the account is deleted from servers in the United States. (A.B. Decl., 7).

The non-content information that remains in the United States when an account is migrated abroad falls into three categories. First, certain non-content information is retained in a data warehouse in the United States for testing and quality control purposes. (A.B. Decl., 10). Second, Microsoft retains "address book" information relating to certain web-based e-mail accounts in an "address book clearing house." (A.B. Decl., 10). Finally, certain basic non-content information about all accounts, such as the user's name and country, is maintained in a database in the United States. (A.B. Decl., 10).

On December 4, 2013, in response to an application by the United States, I issued the search warrant that is the subject of the instant motion. That warrant authorizes 468*468 the search and seizure of information associated with a specified web-based e-mail account that is "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA." (Search and Seizure Warrant ("Warrant"), attached as Exh. 1 to Declaration of CD. dated Dec. 17, 2013 ("CD. Decl."), Attachment A). The information to be disclosed by Microsoft pursuant to the warrant consists of:

> a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
>
> b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
>
> c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
>
> d. All records pertaining to communications between MSN ... and any person regarding the account, including contacts with support services and records of actions taken.

(Warrant, Attachment C, I(a)-(d)).

It is the responsibility of Microsoft's Global Criminal Compliance ("GCC") team to respond to a search warrant seeking stored electronic information. (CD. Decl., 3). Working from offices in California and Washington, the GCC team uses a database program or "tool" to collect the data. (CD. Decl., 3, 4). Initially, a GCC team member uses the tool to determine where the data for the target account is stored and then collects the information remotely from the server where the data is located, whether in the United States or elsewhere. (CD. Decl., 5, 6).

In this case, Microsoft complied with the search warrant to the extent of producing the non-content information stored on servers in the United States. However, after it determined that the target account was hosted in Dublin and the content information stored there, it filed the instant motion seeking to quash the warrant to the extent that it directs the production of information stored abroad.

Statutory Framework

The obligation of an Internet Service Provider ("ISP") like Microsoft to disclose to the Government customer information or records is governed by the Stored Communications Act (the "SCA"), passed as part of the Electronic Communications Privacy Act of 1986 (the "ECPA") and codified at 18 U.S.C. §§ 2701-2712. That statute authorizes the Government to seek information by way of subpoena, court order, or warrant. The instrument law enforcement agents utilize dictates both the showing that must be made to obtain it and the type of records that must be disclosed in response.

First, the Government may proceed upon an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." 18 U.S.C. § 2703(b)(1)(B)(i). In response, the service provider must produce (1) basic customer information, such as the customer's name, address, Internet Protocol connection records, and means of payment for the account, 18 U.S.C. § 2703(c)(2); unopened e-mails that are more than 180 days old, 18 U.S.C. 469*469 § 2703(a); and any opened e-mails, regardless of age, 18 U.S.C. § 2703(b)(1)(B)(i).[2] The usual standards for issuance of compulsory process apply, and the SCA does not impose any additional requirements of probable cause or reasonable suspicion. However, the Government may obtain by subpoena the content of e-mail only if prior notice is given to the customer. 18 U.S.C. § 2703(b)(1)(B)(i).

If the Government secures a court order pursuant to 18 U.S.C. § 2703(d), it is entitled to all of the information subject to production under a subpoena and also "record[s] or other information pertaining to a subscriber [ ] or customer," such as historical logs showing the e-mail addresses with which the customer had communicated. 18 U.S.C. § 2703(c)(1). In order to obtain such an order, the Government must provide the court with "specific and articulable facts showing that there are reasonable grounds to believe that the content of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d).

470*470 Finally, if the Government obtains a warrant under section 2703(a) (an "SCA Warrant"), it can compel a service provider to disclose everything that would be produced in response to a section 2703(d) order or a subpoena as well as unopened e-mails stored by the provider for less than 180 days. In order to obtain an SCA Warrant, the Government must "us[e] the procedures described in the Federal Rules of Criminal Procedure" and demonstrate probable cause. 18 U.S.C. § 2703(a); *see* Fed.R.Crim.P. 41(d)(1) (requiring probable cause for warrants).

Discussion

Microsoft's argument is simple, perhaps deceptively so. It notes that, consistent with the SCA and Rule 41 of the Federal Rules of Criminal Procedure, the Government sought information here by means of a warrant. Federal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States. Therefore, Microsoft concludes, to the extent that the warrant here requires acquisition of information from Dublin, it is unauthorized and must be quashed.

That analysis, while not inconsistent with the statutory language, is undermined by the structure of the SCA, by its legislative history, and by the practical consequences that would flow from adopting it.

A. *Statutory Language*

In construing federal law, the "starting point in discerning congressional intent is the existing statutory language." *Lamie v. United States Trustee,* 540 U.S. 526, 534, 124 S.Ct. 1023, 157 L.Ed.2d 1024 (2004) (citing *Hughes Aircraft Co. v. Jacobson,* 525 U.S. 432, 438, 119 S.Ct. 755, 142 L.Ed.2d 881 (1999)). "And where the statutory language provides a clear answer, [the analysis] ends there as well." *Hughes Aircraft Co.,* 525 U.S. at 438, 119 S.Ct. 755 . However, a court must search beneath the surface of text that is ambiguous, that is, language that is "capable of being understood in two or more possible senses or ways." *Chickasaw Nation v. United States,* 534 U.S. 84, 90, 122 S.Ct. 528, 151 L.Ed.2d 474 (2001) (internal quotation marks omitted).

Here, the relevant section of the SCA provides in pertinent 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.

18 U.S.C. § 2703(a). This language is ambiguous in at least one critical respect. The words "using the procedures described in the Federal Rules of Criminal Procedure" could be construed to mean, as Microsoft argues, that all aspects of Rule 41 are incorporated by reference in section 2703(a), including limitations on the territorial reach of a warrant issued under that rule. But, equally plausibly, the statutory language could be read to mean that while procedural aspects of the application process are to be drawn from Rule 41 (for example, the presentation of the application based on sworn testimony to a magistrate judge), more substantive rules are derived from other sources. *See In re United States,* 665 F.Supp.2d at 1219 (finding ambiguity in that "`[i]ssued' may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as a shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41"); *In re Search of Yahoo, Inc.,* No. 471*471 07-3194, 2007 WL 1539971, at *5 (D.Ariz. May 21, 2007) (finding that "the phrase `using the procedures described in' the Federal Rules remains ambiguous"). In light of this ambiguity, it is appropriate to look for guidance in the "statutory structure, relevant legislative history, [and] congressional purposes." *Florida Power & Light Co. v. Lorion,* 470 U.S. 729, 737, 105 S.Ct. 1598, 84 L.Ed.2d 643 (1985); *see Board of Education v. Harris,* 444 U.S. 130, 140, 100 S.Ct. 363, 62 L.Ed.2d 275 (1979); *Hall v. EarthLink Network, Inc.,* 396 F.3d 500, 504 (2d Cir.2005) .

B. *Structure of the SCA*

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.

> Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime. When we use a computer network such as the Internet, however, a user does not have a physical "home," nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a "virtual home," in fact that "home" is really just a block of ones and zeroes stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.

> This feature of the Internet's network architecture has profound consequences for how the Fourth Amendment protects Internet communications—or perhaps more accurately, how the Fourth Amendment may not protect such communications much at all.
>
> *See* Kerr, *A User's Guide* at 1209-10 (footnotes omitted).

Accordingly, the SCA created "a set of Fourth Amendment—like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." *Id.*at 1212. Because there were no constitutional limits on an ISP's disclosure of its customer's data, and because the Government could likely obtain such data with a subpoena that did not require a showing of probable cause, Congress placed limitations on the service providers' ability to disclose information and, at the same time, defined the means that the Government could use to obtain it. *See id.* at 1209-13.

In particular, the SCA authorizes the Government to procure a warrant requiring a provider of electronic communication service to disclose e-mail content in the provider's electronic storage. Although section 2703(a) uses the term "warrant" and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question.

472*472 This unique structure supports the Government's view that the SCA does not implicate principles of extraterritoriality. 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. *See Marc Rich & Co., A.G. v. United States,* 707 F.2d 663, 667 (2d Cir.1983) ("Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location." (citations omitted)); *Tiffany (NJ) LLC v. Qi Andrew,* 276 F.R.D. 143, 147-48 (S.D.N.Y.2011) ("If the party suboenaed has the practical ability to obtain the documents, the actual physical location of the documents—even if overseas—is immaterial."); *In re NTL, Inc. Securities Litigation,* 244 F.R.D. 179, 195 (S.D.N.Y. 2007); *United States v. Chase Manhattan Bank, N.A.,* 584 F.Supp. 1080, 1085 (S.D.N.Y.1984). To be sure, the "warrant" requirement of section 2703(a) cabins the power of the government by requiring a showing of probable cause not required for a subpoena, but it does not alter the basic principle that an entity lawfully obligated to produce information must do so regardless of the location of that information.

This approach is also consistent with the view that, in the context of digital information, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer." Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L.Rev. 531, 551 (2005). In this case, no such exposure takes place until the information is reviewed in the United States, and consequently no extraterritorial search has occurred.

This analysis is not undermined by the Eighth Circuit's decision in *United States v. Bach,* 310 F.3d 1063 (8th Cir.2002). There, in a footnote the court noted that "[w]e analyze this case under the search warrant standard, not under the subpoena standard. While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants." *Id.* at 1066 n. 1. Given the context in which it was issued, this sweeping statement is of little assistance to Microsoft. The issue in *Bach* was whether the fact that a warrant for electronic information was executed by employees of the ISP outside the supervision of law enforcement personnel rendered the search unreasonable in violation of the Fourth Amendment. *Id.* at 1065. The court utilized the stricter warrant standard for evaluating the reasonableness of the execution of a search, as opposed to the standard for executing a subpoena; this says nothing about the territorial reach of an SCA Warrant.

C. *Legislative History*

Although scant, the legislative history also provides support for the Government's position. When the SCA was enacted as part of the ECPA, the Senate report, although it did not address the specific issue of extraterritoriality, reflected an understanding that information was being maintained remotely by third-party entities:

> The Committee also recognizes that computers are used extensively today for the processing and

> storage of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers 473*473 to obtain sophisticated data processing services.... [B]ecause it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.

S.Rep. No. 99-541, at 3 (1986).

While the House report did address the territorial reach of the law, it did so ambiguously. Because the ECPA amended the law with respect to wiretaps, the report notes:

> By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example it ... regulates only those "interceptions" conducted within the territorial United States. Similarly, the controls in Section 201 of the Act [which became the SCA] regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States.

H.R. Rep. 99-647, at 32-33 (1986) (citations omitted). While this language would seem to suggest that information stored abroad would be beyond the purview of the SCA, it remains ambiguous for two reasons. First, in support of its observation that the ECPA does not regulate activities outside the United States, the Committee cited *Stowe v. Devoy,* 588 F.2d 336 (2d Cir.1978). In that case, the Second Circuit held that telephone calls intercepted in Canada by Canadian authorities were admissible in a criminal proceeding even if the interception would have violated Title III of the Omnibus Crime Control Act of 1968 if it had occurred in the United States or been performed by United States officials. *Id.* at 340-41. This suggests that Congress was addressing not the reach of government authority, but rather the scope of the individual rights created by the ECPA. Second, in referring to "access" to stored electronic communications, the Committee did not make clear whether it meant access to the location where the electronic data was stored or access to the location of the ISP in possession of the data.

Additional evidence of congressional intent with respect to this latter issue can be gleaned from the legislative history of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "Patriot Act"). Section 108 of the Patriot Act provided for nationwide service of search warrants for electronic evidence. The House Committee described the rationale for this as follows:

> Title 18 U.S.C. § 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section does not affect the requirement for a search warrant, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet. Currently, Federal Rules of Criminal Procedure 41 requires that the "warrant" be obtained "within the district" where the property is located. An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors and judges in the district in California where the ISP is located to obtain the warrant to search. These time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned.
>
> 474*474 Section 108 amends § 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located.

H.R. Rep. 107-236(1), at 58 (2001). This language is significant, because it equates "where the property is located" with the location of the ISP, not the location of any server. *See In re Search of Yahoo, Inc.,* 2007 WL 1539971, at *4("Commentators have suggested that one reason for the amendments effected by Section 220 of the Patriot Act was to alleviate the burden placed on federal district courts in the Eastern District of Virginia and the Northern District of California where major internet service providers [ ] AOL and Yahoo, respectively, are located.") (citing, *inter alia,* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens,* 72 Geo. Wash. L.Rev. 1375, 1454 (2004)).

Congress thus appears to have anticipated that an ISP located in the United States would be obligated to respond to a warrant issued pursuant to section 2703(a) by producing information within its control,

regardless of where that information was stored.[3]

D. *Practical Considerations*

If the territorial restrictions on conventional warrants applied to warrants issued under section 2703(a), the burden on the Government would be substantial, and law enforcement efforts would be seriously impeded. If this were merely a policy argument, it would be appropriately addressed to Congress. But it also provides context for understanding congressional intent at the outset, for it is difficult to believe that, in light of the practical consequences that would follow, Congress intended to limit the reach of SCA Warrants to data stored in the United States.

First, a service provider is under no obligation to verify the information provided by a customer at the time an e-mail account is opened. Thus, a party intending to engage in criminal activity could evade an SCA Warrant by the simple expedient of giving false residence information, thereby causing the ISP to assign his account to a server outside the United States.

Second, if an SCA Warrant were treated like a conventional search warrant, it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty ("MLAT"). As one commentator has observed, "This process generally remains slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other." Orin S. Kerr, *The Next Generation Communications Privacy Act,* 162 U. Penn. L.Rev. 373, 409 (2014). Moreover, nations that enter into MLATs nevertheless generally retain the discretion to decline a request for assistance. For example, the MLAT between the United States and Canada provides that "[t]he Requested State may deny assistance to the extent that ... execution of the request is contrary to its public interest as determined by its Central Authority." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Can., March 18, 1985, 24 I.L.M. 1092 ("U.S.-Can.MLAT"), Art. V(1). Similarly, the MLAT between 475*475 the United States and the United Kingdom allows the Requested State to deny assistance if it deems that the request would be "contrary to important public policy" or involves "an offense of a political character." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-U.K., Jan. 6, 1994, S. Treaty Doc. No. 104-2 ("U.S.-U.K.MLAT"), Art. 3(1)(a) & (c)(i). Indeed, an exchange of diplomatic notes construes the term "important public policy" to include "a Requested Party's policy of opposing the exercise of jurisdiction which is in its view extraterritorial and objectionable." Letters dated January 6, 1994 between Warren M. Christopher, Secretary of State of the United States, and Robin W. Renwick, Ambassador of the United Kingdom of Great Britain and Northern Ireland (attached to U.S.-U.K. MLAT). Finally, in the case of a search and seizure, the MLAT in both of these examples provides that any search must be executed in accordance with the laws of the Requested Party. U.S.-Can. MLAT, Art. XVI(1); U.S.-U.K. MLAT, Art. 14(1), (2). This raises the possibility that foreign law enforcement authorities would be required to oversee or even to conduct the acquisition of information from a server abroad.

Finally, as burdensome and uncertain as the MLAT process is, it is entirely unavailable where no treaty is in place. Although there are more than 60 MLATs currently in force, Amy E. Pope, *Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches,* 65 Fla. L.Rev.1917, 1931 (2013), not all countries have entered into such agreements with the United States. Moreover, Google has reportedly explored the possibility of establishing true "off-shore" servers: server farms located at sea beyond the territorial jurisdiction of any nation. Steven R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law,* 43 U. Conn. L.Rev. 709, 716-18 (2011). Thus, under Microsoft's understanding, certain information within the control of an American service provider would be completely unavailable to American law enforcement under the SCA.[4]

The practical implications thus make it unlikely that Congress intended to treat a Section 2703(a) order as a warrant for the search of premises located where the data is stored.

E. *Principles of Extraterrioriality*

The presumption against territorial application

> provides that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none, *Morrison v. National Australia Bank Ltd.,* 561 U.S. 247, 255, 130 S.Ct. 2869, 2878, 177 L.Ed.2d 535 (2010), and reflect the "presumption that United States law governs domestically but does not rule the world," *Microsoft Corp. v. AT & T Corp.,* 550 U.S. 437, 454, 127 S.Ct. 1746, 167 L.Ed.2d 737 (2007) .

Kiobel v. Royal Dutch Petroleum Co., ___ U.S. ___, ___, 133 S.Ct. 1659, 1664, 185 L.Ed.2d 671 (2013) . But the concerns that animate the presumption against extraterritoriality are simply not present here: an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service

provider employees at the location where data are stored. At least in this 476*476 instance, it places obligations only on the service provider to act within the United States. Many years ago, in the context of sanctioning a witness who refused to return from abroad to testify in a criminal proceeding, the Supreme Court observed:

> With respect to such an exercise of authority, there is no question of international law, but solely of the purport of the municipal law which establishes the duty of the citizen in relation to his own government. While the legislation of the Congress, unless the contrary intent appears, is construed to apply only within the territorial jurisdiction of the United States, the question of its application, so far as citizens of the United States are concerned, is one of construction, not of legislative power.

Blackmer v. United States, 284 U.S. 421, 437, 52 S.Ct. 252, 76 L.Ed. 375 (1932) (footnotes omitted). Thus, the nationality principle, one of the well-recognized grounds for extension of American criminal law outside the nation's borders, *see**Marc Rich,* 707 F.2d at 666 (citing *Introductory Comment to Research on International Law, Part II, Draft Convention on Jurisdiction With Respect to Crime,*29 Am. J. Int'l Law 435, 445 (Supp.1935)), supports the legal requirement that an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation.

The cases that Microsoft cites for the proposition that there is no authority to issue extraterritorial warrants are inapposite, since these decisions refer to conventional warrants. For example, in *United States v. Odeh,* 552 F.3d 157 (2d Cir.2008), the Second Circuit noted that "seven justices of the Supreme Court [in *United States v. Verdugo-Urquidez,* 494 U.S. 259, 110 S.Ct. 1056, 108 L.Ed.2d 222 (1990)] endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches," *id.* at 169, and found that "it is by no means clear that U.S. judicial officers could be authorized to issue warrants for overseas searches," *id.* at 171. But *Odeh* involved American law enforcement agents engaging in wiretapping and searching a residence in Kenya. *Id.* at 159-60. The court held that while the Fourth Amendment's proscription against unreasonable search and seizure would apply in such circumstances, the requirement of a warrant would not. *Id.* at 169-71. Similarly, in *Verdugo-Urquidez,* the Supreme Court held that a Mexican national could not challenge, on Fourth Amendment grounds, the search of his residence in Mexico by American agents acting without a warrant. 494 U.S. at 262-63, 274-75, 110 S.Ct. 1056 ; *id.* at 278, 110 S.Ct. 1056 (Kennedy, J., concurring); *id.* at 279, 110 S.Ct. 1056 (Stevens, J., concurring). Those cases are not applicable here, where the requirement to obtain a section 2703(a) order is grounded in the SCA, not in the Warrant Clause.

Nor do cases relating to the lack of power to authorize intrusion into a foreign computer support Microsoft's position. In *In re Warrant to Search a Target Computer at Premises Unknown,* 958 F.Supp.2d 753 (S.D.Tex.2013), the court rejected the Government's argument that data surreptitiously seized from a computer at an unknown location would be "located" within the district where the agents would first view it for purposes of conforming to the territorial limitations of Rule 41. *Id.* at 756-57. But there the Government was not seeking an SCA Warrant.

> The Government [did] not seek a garden-variety search warrant. Its application request[ed] authorization to surreptitiously install data extraction software on the Target Computer. Once installed, the software [would have] the capacity 477*477 to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district.

Id. at 755. "In other words, the Government [sought] a warrant to hack a computer suspected of criminal use." *Id.* Though not "garden-variety," the warrant requested there was conventional: it called for agents to intrude upon the target's property in order to obtain information; it did not call for disclosure of information in the possession of a third party. Likewise, in *United States v. Gorshkov,* No. CR 00-550, 2001 WL 1024026 (W.D.Wash. May 23, 2001), government agents seized a computer in this country, extracted a password, and used it to access the target computer in Russia. *Id.* at *1. The court characterized this as "extraterritorial access" to the Russian computer, and held that "[u]ntil the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment." *Id.* at *3. But this case is of even less assistance to Microsoft since the court did not suggest that it would have been beyond a court's authority to issue a warrant to accomplish the same result.[5]

Perhaps the case that comes closest to supporting Microsoft is *Cunzhu Zheng v. Yahoo! Inc.,* No. C-08-1068, 2009 WL 4430297 (N.D.Cal. Dec. 2, 2008), because at least it deals with the ECPA. There, the plaintiffs sought damages against an ISP on the ground that it had provided user information about them to the People's Republic of China (the "PRC") in violation of privacy provisions of the ECPA and particularly of the SCA. *Id.* at

*1. The court found that "the alleged interceptions and disclosures occurred in the PRC," *id.* at *4, and as a result, dismissed the action on the ground that "[p]laintiffs point to no language in the ECPA itself, nor to any statement in the legislative history of the ECPA, indicating Congress intended that the ECPA ... apply to activities occurring outside the United States," *id.* at *3. But this language, too, does not advance Microsoft's cause. The fact that protections against "interceptions and disclosures" may not apply where those activities take place abroad hardly indicates that Congress intended to limit the ability of law enforcement agents to obtain account information from domestic service providers who happen to store that information overseas.

Conclusion

Even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law. Accordingly, Microsoft's motion to quash in part the warrant at issue is denied.

SO ORDERED.

[1] Pursuant to an application by Microsoft, certain information that is commercially sensitive, including the identity of persons who submitted declarations, has been redacted from public filings.

[2] The distinction between opened and unopened e-mail does not appear in the statute. Rather, it is the result of interpretation of the term "electronic storage," which affects whether the content of an electronic communication is subject to rules for a provider of electronic communications service ("ECS"), 18 U.S.C. § 2703(a), or those for a provider of remote computing service ("RCS"), 18 U.S.C. § 2703(b). The SCA regulates the circumstances under which "[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...." 18 U.S.C. § 2703(a). "Electronic storage" is in turn defined as "(A) any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17). While most courts have held that an e-mail is no longer in electronic storage once it has been opened by the recipient, *see, e.g., Crispin v. Christian Audigier, Inc.,*717 F.Supp.2d 965, 987 (C.D.Cal.2010); *United States v. Weaver,* 636 F.Supp.2d 769, 771-73 (C.D.Ill.2009); *see also* Owen S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L.Rev. 1208, 1216 (2004) (hereinafter *A User's Guide*) ("The traditional understanding has been that a copy of an opened e-mail sitting on a server is protected by the RCS rules, not the ECS rules"), the Ninth Circuit has instead focused on whether "the underlying message has expired in the normal course," *Theofel v. Farey-Jones,* 359 F.3d 1066, 1076 (9th Cir. 2004); *see also id.* at 1077 ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage."). Resolution of this debate is unnecessary for purposes of the issue before me.

Likewise, it is not necessary to determine whether Microsoft was providing ECS or RCS in relation to the communications in question. The statute defines ECS as "any service which provides users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), while RCS provides "to the public [ ] computer storage or processing services by means of an electronic communications system, 18 U.S.C. § 2711(2)." Since service providers now generally perform both functions, the distinction, which originated in the context of earlier technology, is difficult to apply. *SeeCrispin,* 717 F.Supp.2d at 986 n. 42; *In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant,* 665 F.Supp.2d 1210, 1214 (D.Or. 2009) (hereinafter *In re United States*) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself."); Kerr, *A User's Guide* at 1215 ("The distinction of providers of ECS and RCS is made somewhat confusing by the fact that most network service providers are multifunctional. They can act as providers of ECS in some contexts, providers of RCS in some contexts, and as neither in some contexts as well.").

[3] Suppose, on the contrary, that Microsoft were correct that the territorial limitations on a conventional warrant apply to an SCA warrant. Prior to the amendment effected by the Patriot Act, a service provider could have objected to a warrant issued by a judge in the district where the provider was headquartered on the basis that the information sought was stored on a server in a different district, and the court would have upheld the objection and quashed the subpoena. Yet, I have located no such decision.

[4] Non-content information, opened e-mails, and unopened e-mails stored more than 180 days could be obtained, but only by means of a subpoena with notice to the target; unopened e-mails stored less than 180 days could not be obtained at all.

[5] Microsoft argues that the Government itself recognized the extraterritorial nature of remote computer searches when it sought an amendment to Rule 41 in 2013. *See* Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division to Hon. Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) ("Raman Letter") at 4-5, *available at* http://uscourts.gov/ uscourts/RulesAndPolicies/. But the proposed amendment had nothing to do with SCA Warrants directed to service providers and, rather, was intended to facilitate the kind of "warrant to hack a computer" that was quashed in *In re Warrant to Search a Target Computer at Premises Unknown*; indeed, the Government explicitly referred to that case in its proposal. Raman Letter at 2.

End of Document.