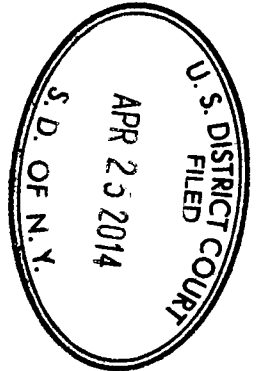UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
█████████@MSN.COM, which is
controlled by Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

**MEMORANDUM IN SUPPORT OF MICROSOFT'S MOTION TO VACATE IN PART
AN SCA WARRANT SEEKING CUSTOMER INFORMATION LOCATED OUTSIDE
THE UNITED STATES**

TABLE OF CONTENTS

Page(s)

CASES

On December 4, 2013, this Court, on application of the United States, issued a search warrant directed at Microsoft Corporation ("Microsoft") seeking customer data that, with the exception of certain non-content and address book information stored domestically, are not located in any form within the United States. Insofar as the warrant may be construed to authorize the search and seizure of data located outside the United States, Microsoft respectfully moves to vacate the warrant as unauthorized to such extent.

Courts in the United States are not authorized to issue warrants for extraterritorial searches and seizures. The result does not change because the warrant at issue here was sought under authority of the Stored Communications Act, 18 U.S.C. § 2703(a) ("SCA"). Although the SCA allows the Government to use a search warrant to obtain stored email communications from electronic communication service providers, it does not empower courts to issue warrants authorizing searches and seizures outside the United States. Nor does the SCA require electronic communication service providers to make available in the United States evidence that is not otherwise within the territorial reach of federal courts' warrant authority.

I. RELEVANT FACTS

The warrant authorizes the search and seizure of information associated with a Microsoft web-based email account named █████@msn.com. Declaration of █████ at ¶ 7, Ex. 1 ("█████ Decl."). The warrant states that information associated with that account is "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA." *Id.* at ¶ 7, Ex. 1 at Attachment A ("Property To Be Searched"). The warrant further requires Microsoft to disclose the following information relating to the account, to the extent such information is "within [Microsoft's] possession, custody, or control":

1. The contents of all emails stored in the account, including copies of emails sent from the account;

2. 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 type of services utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);

3. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

4. All records pertaining to communications between MSN or Yahoo and any person regarding the account, including contacts with support services and records of actions taken.

Id. at ¶ 7, Ex. 1 at Attachment C ("Particular Things To Be Seized").

For many years, Microsoft has owned and operated a free, web-based email service. This service has existed at various times under different internet domain names, including, *inter alia*, Hotmail.com, MSN.com, and (since 2013) Outlook.com. *See* Declaration of ▮▮▮ at ¶ 3 ("▮Decl."). Users of Microsoft web-based email accounts navigate to "Outlook.com" and log on using a username and password. *Id.* Once logged on, the user may send and receive email messages; the user may also store messages in personalized folders. *Id.*

Email message data are made up of two categories of information: (1) content information, *i.e.*, the body of an email and its subject line; and (2) non-content information about the email message, such as the sender address, recipient address, and date and time of transmission. *Id.* at ¶ 4.

Email messages sent and received by users are stored by Microsoft in Microsoft datacenters. To improve service to users, in September 2010, Microsoft began to store data for

certain web-based email accounts in a datacenter in Dublin, Ireland, which is leased and operated by Microsoft's wholly-owned Irish subsidiary, Microsoft Ireland Operations Limited. *Id.* at ¶¶ 5-6. The addition of the Dublin datacenter boosted the quality of service to users located in certain countries, for example, in Europe.[1]

Microsoft stores email account data in the Dublin datacenter ████████████████████ depending on the country in which the user, when registering for email service, indicates he or she is located. ██

██

Several times each day, Microsoft's software performs an automatic scan function to determine, based on the "country code" entered by the user when registering for an account, whether an account should be migrated to the Dublin datacenter. *Id.* Once an account is so migrated, all content and non-content information associated with the account in the United States is marked for deletion and subsequently deleted from Microsoft's servers in the United States.[2] *Id.*

The three exceptions to this framework concern certain non-content information and address book data. First, for testing and quality control purposes, Microsoft operates a "data warehouse" in the United States that stores certain non-content information relating to Microsoft web-based email accounts, including data associated with accounts hosted from the Dublin datacenter. *Id.* at ¶ 10. Second, Microsoft also operates an "address book clearing house" that contains online "address book" information relating to certain web-based email accounts,

---

[1]   As the geographic distance between a user and a datacenter where the user's account is hosted increases, the quality of service decreases—a phenomenon known as "network latency." ██ *See* ██ Decl. at ¶ 6.

[2]   No redundant copies of account data stored in the Dublin datacenter are stored in the United States. *See* ██ Decl. at ¶ 8.

including accounts hosted from Dublin. *Id.* Third, Microsoft maintains a database in the United States containing basic non-content information about web-based email accounts, such as the user's name and country provided during registration. *Id.* To the extent that the warrant calls for the search and seizure of non-content information and address book data for the account described in the warrant (*e.g.*, categories 2-4 of Attachment C of the warrant), Microsoft has delivered the data ("Delivered Data") to the Government contemporaneously with the filing of this motion because that information is stored in the United States. ███ Decl. at ¶ 8, Ex. 2.

The content data associated with the account identified in the warrant are hosted in a datacenter in Dublin, Ireland. A member of Microsoft's Global Criminal Compliance ("GCC") team,[3] located in the United States, made this determination by logging into a database management program ████████████████████ *See id.* at ¶ 7. The GCC team member entered identifying information concerning the account ███████ and determined the location of the user data. *Id.* ████████████████████

███
███
███
███
███
███
███
█████████████████████████████ *Id.*
████████████████████████████

---

[3]   The GCC team handles all responses to search warrants for stored electronic communications data.

II. ARGUMENT

A. Extraterritorial Warrants Are Not Authorized by Rule 41 or any Other Source of Law.

Neither Rule 41 of the Federal Rules of Criminal Procedure, nor any other rule or statute, authorizes the issuance of warrants to be executed outside the territory of the United States. *See United States v. Vilar*, No. 05-CR-621, 2007 WL 1075041, at *52 (S.D.N.Y. Apr. 4, 2007) ("[A]s other courts have observed, there is no statutory basis for a magistrate judge in the Southern District of New York to issue a search warrant in a non-terrorism case targeting property in the Eastern District of New York, let alone to issue such a warrant to be executed in London, England."); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000) (holding that "there is presently no statutory basis for the issuance of a warrant to conduct searches abroad"). Indeed, the Supreme Court expressly rejected a proposed amendment to Rule 41 that would have permitted the issuance of warrants authorizing searches for property outside of the United States. *See* Fed. R. Crim. P. 41, Notes of Advisory Committee on Rules — 1990 Amendment.

In the absence of any rule of procedure or statutory authority, courts have not recognized any inherent authority to issue warrants seeking property outside of the United States. In *United States v. Odeh*, 552 F.3d 157 (2d Cir. 2008), for instance, the Second Circuit observed that "seven justices of the Supreme Court [in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)] endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches," *id.* at 169, and held that "it is by no means clear that U.S. judicial officers *could be* authorized to issue warrants for overseas searches," *id.* at 171 (emphasis added).[4] In *United*

---

[4]   *See Verdugo-Urquidez*, 494 U.S. at 279 (Stevens, J., concurring) ("I do not believe the Warrant Clause has any application to searches of noncitizens' homes in foreign jurisdictions (continued...)

States v. Williams, 617 F.2d 1063 (5th Cir. 1980), the Fifth Circuit, sitting *en banc*, similarly observed that "there is substantial doubt that the federal district courts have the authority to issue [extraterritorial] warrant[s]." *Id.* at 1072; *see also Weinberg v. United States*, 126 F.2d 1004, 1006 (2d Cir. 1942) (observing that "[w]ith very few exceptions, United States district judges possess no extraterritorial jurisdiction," and construing statute authorizing issuance of search warrants as limited by the court's territorial jurisdiction).

The Government itself has recognized it cannot conduct warranted searches outside the United States. In a recent request to amend Rule 41, the Government described its proposed amendment as consistent with the presumption against extraterritoriality and explained that the amendment "does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) at 4-5, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/cr-suggestions-2013/13-CR-B-Suggestion_Raman.pdf. In fact, the Government recognized that even under its proposed amendment, "should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect." *Id.*

This warrant calls for the disclosure of content data that can only be obtained through an extraterritorial search and seizure. ███████████████████████████████

██

_____

because American magistrates have no power to authorize such searches."); *id.* at 278 (Kennedy, J., concurring) (remarking upon the "[t]he absence of local judges or magistrates available to issue [extraterritorial] warrants"); *id.* at 297 (Blackmun, J., dissenting) ("[A]n American magistrate's lack of power to authorize a search abroad renders the Warrant Clause inapplicable to the search of a noncitizen's residence outside this country.").

[REDACTED] In other words, the search and

seizure would take place in Ireland, not the United States. *See, e.g., United States v. Gorshkov,*

No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (holding that federal

agents' "extraterritorial access to computers in Russia" constituted "a search or seizure of . . .

property outside the territory of the United States" (citing *Verdugo-Urquidez,* 494 U.S. 259));[5] *In*

re Warrant to Search a Target Computer at Premises Unknown, No. H-13-234M, 2013 WL

1729765 (S.D. Tex. April 22, 2013) (rejecting Government's application for a search warrant

under Rule 41 where the Government "admits that the current location of the Target Computer is

unknown," and emphasizing that the location of the data — not the location of the searching

agents — determines the location of the search for purposes of Rule 41); *accord* U.S. Dep't of

Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal*

Investigations, at 85 (2009), *available at*

http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf ("When agents learn before

a search that some or all of the data is stored remotely outside of the United States, matters

become more complicated. The United States may be required to take actions ranging from

informal notice to a formal request for assistance to the country concerned," even though "the

search may seem domestic to a U.S. law enforcement officer executing the search in the United

States pursuant to a valid warrant . . . .").

---

[5]   In *Gorshkov,* the Government did not initially obtain a warrant; rather, federal agents in
Seattle surreptitiously obtained the defendant's computer passwords and then used them to
access remotely one of the defendant's computers located in Russia. 2001 WL 1024026, at *1.
The court ultimately rejected the defendant's motion to suppress on the grounds that the Fourth
Amendment did not apply to the agents' extraterritorial search of a non-resident alien's property.
Id. at *3. Because the Government in this case sought and obtained a warrant, the ultimate
question addressed by the court in *Gorshkov* is not presented here.

The warrant was issued under the authority of the SCA presumably on the assumption that all data sought are located in the United States. (As noted above, Microsoft already has produced to the Government the Delivered Data located in the United States.) The content data sought by the warrant, however, are located in Dublin, Ireland. The warrant is not valid to authorize the search and seizure of this evidence.

B. The SCA Does Not Provide an Independent Legal Basis to Obtain Electronic Communications Data Located Outside of the United States.

Nothing in the SCA or its legislative history suggests that it may be used to reach the contents of electronic communications in foreign countries. The scope of the Government's authority to seek content data under the SCA is defined by the valid scope of the warrant at issue. The statute provides that the Government in these circumstances must obtain "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure" (or the procedures provided under applicable state laws). 18 U.S.C. § 2703(a); *see also United States v. Warshak*, 631 F.3d 266, 283 (6th Cir. 2010) ("The government may obtain the contents of e-mails that are in electronic storage with an electronic communication service for 180 days or less only pursuant to a warrant." (internal quotation marks omitted)). The warrant here cannot authorize the search and seizure of property located outside the United States — whether or not the Court issued it under the authority of the SCA.

Moreover, it bears emphasis that Microsoft has received a *warrant* under the SCA, and not a subpoena. The two forms of process are distinct. *See United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) ("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." (citing 18 U.S.C. § 2703(b)(1)(A)). Unlike subpoenas, search warrants may not be used to compel production of evidence located outside the United States if it is

merely within the provider's "possession, custody, or control." Permitting search warrants to be used like subpoenas in this way would effectively vest the Government with power to accomplish indirectly (through the assistance of an electronic communication service provider) what it could not do directly — namely, conduct a warranted extraterritorial search.

In addition, the plain meaning of the SCA does not authorize extraterritorial warrants. As the Supreme Court recently reaffirmed in *Morrison v. National Australia Bank Ltd.*, 130 S. Ct. 2869 (2010), "unless there is the affirmative intention of the Congress clearly expressed to give a statute extraterritorial effect, we must presume it is primarily concerned with domestic conditions." *Id.* at 2877 (internal quotation marks and citation omitted). "When a statute gives no clear indication of an extraterritorial application, it has none." *Id.* at 2878.

Nothing in the SCA's text or legislative history suggests that the law is meant to authorize warrants for extraterritorial searches. Rather, when Congress amended the SCA in 2001 to provide that search warrants could be issued by a magistrate judge with jurisdiction over the offense under investigation, even for electronic data located outside of the judge's district, the very title of the amendment was "*Nation*wide Service of Search Warrants for Electronic Evidence." Pub. L. No. 107-56, § 220, 115 Stat. 272 (2001) (emphasis added); *see also Vilar*, 2007 WL 1075041 at *52 n.33 (observing that "nothing in the language of [the 2001 SCA] amendment remotely suggests that the power [of a magistrate judge to authorize a search outside of his or her district] extended to extraterritorial searches"). The legislative history confirms that this amendment to the SCA "[p]ermits a single court having jurisdiction over the offense to issue a search warrant for e-mail that would be valid . . . *anywhere in the United States*." 147 Cong. Rec. H7159-03 at H7197-98 (emphasis added).

The absence of authority in the SCA for extraterritorial warrants is confirmed by the ruling of at least one federal district court, which explicitly rejected the argument that the Electronic Communications Privacy Act ("ECPA"), which includes the SCA, applies extraterritorially. In *Zheng v. Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 21, 2009), the court held that ECPA does not apply outside the United States, and further noted that Congress had not made clear, through either ECPA's text or legislative history, its intent that the law apply outside the United States. *See id.* *2–4 (internal quotation marks and citation omitted).[6]

Neither does the SCA compel a private electronic communication service provider, such as Microsoft, to cause data outside the United States to be transferred into the United States in response to a search warrant. As the text of the statute makes clear, the recipient of a warrant under the SCA must act upon receipt of a *valid* warrant. A warrant is not valid insofar as it is used for the search and seizure of material outside the United States; thus, under the SCA, no action is required by Microsoft to cause electronic data outside the United States to be transported to the United States.

In short, the SCA does not authorize extraterritorial warrants. Accordingly, insofar as the warrant here may be construed to authorize the search and seizure of data located outside the United States, Microsoft respectfully moves to vacate the warrant to such extent.

---

[6]   Notably, the court in *Zheng* held that ECPA did not apply to interceptions that took place abroad, even if the emails, prior to their disclosure "travelled electronically through a network located in the United States." *Id.* at *4.
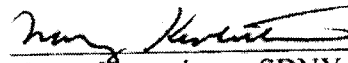
III. CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that the Court vacate that part of the warrant calling for the search and seizure of customer information located outside the United States.

Dated: December 18, 2013

Respectfully submitted,

MICROSOFT CORPORATION

Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkbllp.com
nboxer@pkbllp.com

Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
nkestenbaum@cov.com
ccatalano@cov.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
Fax: 202.662.6291
jgarland@cov.com
aberengaut@cov.com

*Applications for admission pro hac vice
pending

Counsel for Microsoft Corporation