UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation

REDACTED

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

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: JUN 06 2014

MICROSOFT'S OBJECTIONS TO THE MAGISTRATE'S ORDER DENYING MICROSOFT'S MOTION TO VACATE IN PART A SEARCH WARRANT SEEKING CUSTOMER INFORMATION LOCATED OUTSIDE THE UNITED STATES

TABLE OF CONTENTS

Page(s)

I. Introduction and Summary of Argument 1

II. Factual Background and Procedural History 5

A. Microsoft's Web-Based Email Service 5

B. The Government Obtained a Warrant From the Magistrate Judge to Search For and Seize All Content in a Named Email Account. 7

C. The Government Sought to Compel Microsoft to Search for and Seize User Content Located in Dublin on the Government's Behalf. 8

D. Proceedings Before the Magistrate Judge 9

III. Argument 9

A. Neither ECPA Nor Any Other Source of Law Authorizes The Court to Issue a Search Warrant for Information Stored Outside the United States 9

1. ECPA and the Fourth Amendment Require the Government to Obtain a Warrant to Search and Seize the Contents of Email. 9

2. The Term "Warrant" in ECPA Must Be Given its Ordinary Meaning, Including Attendant Limitations. 13

3. ECPA Warrants, Like All Warrants, Are Confined to the Territory of the United States. 16

4. Interpreting ECPA to Authorize Searches and Seizures Outside the United States Would Violate International Law And Raise Serious Foreign Policy Concerns That Congress Presumptively Would Have Sought to Avoid 18

5. The Warrant Purports to Conscript Microsoft to Execute an Invalid Extraterritorial Search and Seizure on the Government's Behalf 21

6. The Magistrate Judge Erred by Concluding That Congress Intended Warrants Issued Under ECPA to Have Global Reach. 22

B. Even if Permitted by ECPA, the Warrant Is Unlawful Because It Violates the Particularity Requirement of the Fourth Amendment to the Constitution. 26

C. The Government Should Seek the Relevant User Information by Following the Process Established by the US-Ireland MLAT 27

IV. Conclusion 30

TABLE OF AUTHORITIES

Page(s)

Cases

ALCOA v. EPA,
663 F.2d 499 (4th Cir. 1981) 9

Hubbard v. Myspace, Inc.,
788 F. Supp. 2d 319 (S.D.N.Y. 2011) 17

In re Application of the United States,
620 F.3d 304 (3d Cir. 2010) 13, 19

In re Subpoena Duces Tecum,
228 F.3d 341 (4th Cir. 2000) 12

In re Warrant to Search a Target Computer at Premises Unknown
No. H-13-234M, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) 16

Katz v. United States,
389 U.S. 347 (1967) 9

Kiobel v. Royal Dutch Petroleum Co.,
133 S. Ct. 1659 (2013) 19

Marc Rich & Co. v. United States,
707 F.2d 663 (2d Cir. 1983) 24

Matter of Search of Information Associated with [Redacted]@mac.com,
--- F. Supp. 2d. ----, 2014 WL 1377793 (D.D.C. 2014) 16, 24

McQuiggin v. Perkins,
133 S. Ct. 1924 (2013) 11

Milner v. Dep't of Navy,
131 S. Ct. 1259 (2011) 22

Mohamad v. Palestinian Authority,
132 S. Ct. 1702 (2012) 13

Morrison v. Nat'l Bank Ltd.,
130 S. Ct. 2869 (2010) 3, 19

Rajaratnam v. Moyer,
47 F.3d 922 (7th Cir. 1995) 9

Skinner v. Ry. Labor Execs' Ass'n,
489 U.S. 602 (1989).....21, 26

United States v. Bach,
310 F.3d 1063 (8th Cir. 2002).....13

United States v. Bansal,
663 F.3d 634 (3d Cir. 2011).....15

United States v. Berkos,
543 F.3d 392 (7th Cir. 2008).....15, 23

United States v. Bin Laden,
126 F. Supp. 2d 264 (S.D.N.Y. 2000).....17

United States v. Blanco,
861 F.2d 773 (2d Cir. 1988).....20

United States v. Clark,
638 F.3d 89 (2d Cir. 2011).....27

United States v. Davis,
767 F.2d 1025 (2d Cir. 1985).....25

United States v. Gorshkov
No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).....16

United States v. Jacobsen,
466 U.S. 109 (1984).....9

United States v. King,
No. 94-CR-455, 1997 WL 582882 (S.D.N.Y. Sept. 19, 1997).....12

United States v. Kyles,
40 F.3d 519 (2d Cir. 1994).....11

United States v. Lemmons,
527 F.2d 662 (6th Cir. 1975).....27

United States v. Magassouba,
544 F.3d 387 (2d Cir. 2008).....27

United States v. Nafzger,
965 F.2d 213 (7th Cir. 1992).....27

United States v. Odeh,
552 F.3d 157 (2d Cir. 2008).....17, 20, 24

United States v. Palestine Liberation Org.,
695 F. Supp. 1456 (S.D.N.Y. 1988).....21

United States v. Thomas,
878 F.2d 383 (6th Cir. 1989).....23

United States v. Van Leeuwen,
397 U.S. 249 (1970).....23

United States v. Vilar,
No. 05-CR-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007).....17, 18

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010).....*passim*

United States v. Warshay,
No. 98–CV–1245, 1998 WL 767138 (E.D.N.Y. Aug. 4, 1998).....9

United States v. Wuagneux,
683 F.2d 1343 (11th Cir. 1982).....26

Weinberger v. Rossi,
456 U.S. 25 (1982).....3, 19

Zheng v. Yahoo! Inc.,
No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009).....19

Statutes and Regulations

18 U.S.C. § 2703(a).....*passim*

18 U.S.C. §2703(b).....10

18 U.S.C. § 2703(b)(1)(B)(i).....11, 12

18 U.S.C. § 2703(d).....13

18 U.S.C. § 2705(a)(1)(B).....12

18 U.S.C. §§ 2711(3)(B).....20

18 U.S.C. § 3109.....11

28 U.S.C. § 636(b)(1)(B)–(C).....9

28 U.S.C. § 636(b)(3).....9

Pub. L. No. 99-508 § 201, 100 Stat. 1861 (1986).....14

Pub. L. No. 107-56 § 220, 115 Stat. 291 (2001) 18

Fed. R. Crim P. 17(c) 12

Fed. R. Crim. P. 17(c)(1) 12

Fed. R. Crim. P. 41(b)(5) 17

Fed. R. Crim. P. 41(d)(1) 12

Fed. R. Crim. P. 41(e) 15, 23

Fed. R. Civ. P. 41(e)(2)(A) 15, 24

Fed. R. Crim. P. 41(e)(2)(B) 16

Fed. R. Crim. P. 41, Notes of Advisory Committee on Rules — 1990 Amendment 17

Other Authorities

Agreement on Mutual Legal Assistance Between the European Union and the United States of America, arts. 3 & 7, June 25, 2003, T.I.A.S. 10-201.1 21

Mutual Legal Assistance Treaty Between the United States of America and Ireland, art. 14, T.I.A.S. 13137, Jan. 18, 2001. 20

Vienna Convention on the Law of Treaties art. 27, May 22, 1969 20

Law Enforcement Treaties: Hearing Before the Committee on Foreign Relations of the U.S. Senate, 107th Cong. 19 (2002) 28-29

H.R. Rep. 107-236 (2001) 14, 15

H.R. Rep. 99-647 (1986) 10, 14, 23

S. Rep. 99-541 (1986) 14

147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) 15, 18, 19

RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 432(2) 20, 25

BLACK'S LAW DICTIONARY 1470 (9th ed. 2009) 11

BLACK'S LAW DICTIONARY 1563 (9th ed. 2009) 12

Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700 (2010) 16

I. Introduction and Summary of Argument

The Magistrate Judge issued a warrant under the Electronic Communications Privacy Act ("ECPA") that, on its face, purports to authorize the Government to search any and all of Microsoft's facilities worldwide. Microsoft moved to vacate the warrant because the private email communications the Government seeks are located in a Microsoft facility in Dublin, Ireland and because Congress has not authorized the issuance of warrants that reach outside U.S. territory. The Government cannot seek and a court cannot issue a warrant allowing federal agents to break down the doors of Microsoft's Dublin facility. Likewise, the Government cannot conscript Microsoft to do what it has no authority itself to do — *i.e.*, execute a warranted search abroad. To end-run these points, the Government argues, and the Magistrate Judge held, that the warrant required by ECPA is not a "warrant" at all. They assert that Congress did not mean "warrant" when using that term, but instead meant some previously unheard of "hybrid" between a warrant and subpoena *duces tecum*. The Government takes the extraordinary position that by merely serving such a warrant on any U.S.-based email provider, it has the right to obtain the private emails of any subscriber, no matter where in the world the data may be located, and without the knowledge or consent of the subscriber or the relevant foreign government where the data is stored.

This interpretation not only blatantly rewrites the statute, it reads out of the Fourth Amendment the bedrock requirement that the Government must specify the place to be searched with particularity, effectively amending the Constitution for searches of communications held digitally. It would also authorize the Government (including state and local governments) to violate the territorial integrity of sovereign nations and circumvent the commitments made by the United States in mutual legal assistance treaties expressly designed to facilitate cross-border criminal investigations. If this is what Congress intended, it would have made its intent clear in

the statute. But the language and the logic of the statute, as well as its legislative history, show that Congress used the word "warrant" in ECPA to mean "warrant," and not some super-powerful "hybrid subpoena." And Congress used the term "warrant" expecting that the Government would be bound by all the inherent limitations of warrants, including the limitation that warrants may not be issued to obtain evidence located in the territory of another sovereign nation.

The Government's interpretation ignores the profound and well established differences between a warrant and a subpoena. A warrant gives the Government the power to seize evidence without notice or affording an opportunity to challenge the seizure in advance. But it requires a specific description (supported by probable cause) of the thing to be seized and the place to be searched — and that place must be in the United States. A subpoena *duces tecum*, on the other hand, does not authorize a search and seizure of the private communications of a third party. Rather, it gives the Government the power to require a person to collect items within her possession, custody, or control, regardless of location, and bring them to court at an appointed time. It also affords the recipient an opportunity to move in advance to quash. Here, the Government wants to exploit the power of a warrant and the sweeping geographic scope of a subpoena, without having to comply with fundamental protections provided by either. There is not a shred of support in the statute or its legislative history for the proposition that Congress intended to allow the Government to mix and match like this. In fact, Congress recognized the basic distinction between a warrant and a subpoena in ECPA when it authorized the Government to obtain certain types of data with a subpoena or a "court order," but required a warrant to obtain a person's most sensitive and constitutionally protected information — the contents of emails less than 6 months old.

Microsoft asks the Court to give effect to the statute's plain meaning. Ignoring the plain meaning of "warrant" would lead the Court down two paths, with serious and far-reaching consequences that should be avoided. First, the Government's interpretation would yield violations of international law and U.S. treaty obligations. The United States and Ireland are close allies that have painstakingly negotiated a Mutual Legal Assistance Treaty ("MLAT") allowing either nation to obtain through a cooperative process precisely the kind of information the Government seeks unilaterally in this case. Allowing warrants issued under ECPA the sweep urged by the Government would violate international law and treaties, and reduce the privacy protection of everyone on the planet. Nothing in the statute indicates that Congress had any such intent, and a statute "ought never to be construed to violate the law of nations, if any other possible construction remains." *Weinberger v. Rossi*, 456 U.S. 25, 32 (1982). If Congress intended the warrant provision in ECPA to have extraterritorial effect, it must give clear indication of that intent, and it has not. *Morrison v. Nat'l Bank Ltd.*, 130 S. Ct. 2869, 2878 (2010). The Government's position, if upheld, will end up harming U.S. citizens' privacy interests because it will invite prosecutors abroad to conduct themselves in the same way, ignore treaty obligations, and serve some form of unilateral process on Microsoft in their countries to obtain U.S. citizens' data stored in the United States.

Second, and contrary to yet another fundamental maxim of statutory construction, the Government asks the Court to interpret ECPA in a manner that would violate the Fourth Amendment's particularity requirement. Specifically, the Government urges the Court to construe a search warrant for email content under ECPA as something much *less* than a search warrant in any other sense. When the Government obtains the contents of email communications, it is conducting a "search" (by definition) for purposes of the Fourth Amendment. That requires a

warrant. In *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), the Court of Appeals for the Sixth Circuit expanded the warrant requirement in ECPA to the content of all email communications, including those held for more than 180 days. Analogizing email to letters and telephone conversations, the court held that emails stored by electronic communication providers are entitled to a reasonable expectation of privacy, and that any effort by government to infringe upon that expectation constituted a search for purposes of the Fourth Amendment. *Warshak*, 631 F.3d at 286.[1] Thus, a warrant served under ECPA is a "warrant" in every sense, and must be consistent with the Fourth Amendment for all purposes, and not just those that are convenient for the Government.

The Warrant in this case violates the Fourth Amendment because it fails to identify the place to be searched with particularity.[2] Instead, the Warrant purports to authorize law enforcement officers to search for any information associated with the target email account that is "stored at premises owned, maintained, controlled, or operated" by Microsoft *anywhere in the world*, and further seeks to conscript Microsoft to execute it on their behalf. That language would empower the Government to search every one of the hundreds of buildings Microsoft owns, controls, or otherwise maintains — which makes it precisely the type of "general" warrant the Fourth Amendment sought to prohibit.

If the Warrant did identify the place to be searched as Microsoft's datacenter in Ireland, it would simply highlight its impermissible scope. The Magistrate Judge could no more have authorized that search than he could authorize a search of a customer's personal letters and effects

---

[1] The Government did not appeal the *Warshak* decision and has consistently followed its holding and obtained search warrants to search for and seize email content since that time.

[2] We presume also that the Warrant is defective because the sealed affidavit supporting probable cause fails to describe with particularity the location of the email content to be seized.

located in a bank safety deposit box in Dublin by issuing a warrant directed at the bank's headquarters in New York. Yet, with this Warrant, the Government asserts that the Court should apply different rules to datacenters (which will house the vast majority of private documents created in the 21st Century) than it has applied to other *locations* for more than two hundred years.

The Government's position, if adopted, will ultimately have a significant negative impact on Microsoft's business, and the competitiveness of U.S. cloud providers in general. Foreign governments and companies have placed their trust in Microsoft and other U.S. cloud providers to safeguard their private documents. Over the course of the past year, Microsoft and other U.S. technology companies have faced growing mistrust and concern about their ability to protect the privacy of personal information located outside the United States. The Government's position in this case further erodes that trust, and will ultimately erode the leadership of U.S. technology companies in the global market.

II. Factual Background and Procedural History

A. Microsoft's Web-Based Email Service

1. Microsoft operates a free, web-based email service that has at various times existed under different internet domain names, including Hotmail.com, MSN.com, and Outlook.com. (Decl. of A.B., dated Dec. 17, 2013, Dkt. 95 ("A.B. Decl."), at ¶ 3.) Microsoft stores email message data associated with this service in its datacenters. (*Id.* at ¶ 5.) This data includes both content information (*i.e.*, the substance of an email and its subject line) and non-content information (*i.e.*, the sender's email address, recipient's email address, and the date and time of transmission). (*Id.* at ¶ 4.) REDACTED

(Decl. of A.B., dated May 29, 2014, at ¶ 5.)

2. 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. (A.B. Decl., at ¶ 5.) The addition of the Dublin datacenter boosted the quality of service to numerous users because it reduces "network latency" — *i.e.*, the inverse ratio between quality of service and the distance between a user and the datacenter where that user's account is hosted. (*Id.* at ¶ 6.) Maximizing quality of service by minimizing network latency is critical to Microsoft's business. The Dublin datacenter allows Microsoft to reduce network latency and improve the quality of service for users located closer to Ireland than to the United States. For Outlook.com accounts stored in Dublin, the users' content resides on a specific server in the Dublin datacenter. It does not exist in any form inside the United States. (*Id.* at ¶ 9.) Certain *non-content* information and address book data, in contrast, is stored in the United States.[3]

3. When Microsoft receives a search warrant for Outlook.com customer information, Microsoft's Global Criminal Compliance ("GCC") team handles the response. (Decl. of C.D., dated Dec. 17, 2013, Dkt. 96 ("C.D. Decl."), at ¶ 3.) To collect the content sought by a search warrant, a GCC team member first must determine the location of the Microsoft server on which the requested data is stored. (*Id.* at ¶ 5.) REDACTED

[redacted] (*Id.* at ¶ 6.)

REDACTED

[3] Three types of data associated with Dublin-based accounts are stored inside the United States. *First*, for testing and quality control purposes, Microsoft operates a data warehouse in the United States that stores certain non-content information relating to web-based email accounts. (A.B. Decl., at ¶ 10.) *Second*, Microsoft operates an address book clearing house in the United States that maintains "address book" information relating to certain web-based email accounts. (*Id.*) *Third*, Microsoft maintains a U.S.-based database of basic subscriber information including the user's name and country provided during registration. (*Id.*)

REDACTED

[redacted] (*Id.*)[4]

In addition to the GCC team in the United States, Microsoft also has employees in Dublin who respond to requests from the Irish Government. (Decl. of REDACTED, dated June 3, 2014 ("REDACTED Decl.").) When the Irish Government seeks Outlook.com data, Microsoft employees in Ireland ascertain where the account data is located. (REDACTED Decl., at ¶¶ 3–5.) For such data stored in Ireland, Microsoft produces the data directly to Irish authorities in compliance with valid Irish legal process. (*Id.* at ¶¶ 5–6.) When the Irish Government seeks data stored in the United States, Microsoft refers the relevant Irish authorities to the United States-Ireland MLAT, which allows the Irish Government to seek data through the U.S. Department of Justice. (*Id.* at ¶ 5.)

B. The Government Obtained a Warrant From the Magistrate Judge to Search For and Seize All Content in a Named Email Account.

On December 4, 2013, upon application of the United States, the Magistrate Judge issued a warrant to search for and seize information associated with a Microsoft web-based email account. (C.D. Decl., at ¶ 7 & Ex. 1 ("Warrant").) The Warrant issued is a standard form AO-93 "Search and Seizure Warrant," the same form used throughout the federal courts to authorize searches and seizures of physical property. (Warrant, at 2.) The Warrant is addressed "To: Any authorized law enforcement officer" and states "YOU ARE COMMANDED to execute this warrant . . . in the daytime 6:00 a.m. to 10:00 p.m." and "authorize[s] the officer executing this warrant to delay notice to the person who . . . will be searched or seized" for 30 days. (*Id.*)

---

[4] The Warrant is not dependent on Microsoft's use of direct access to data stored in Dublin from the United States. This method of obtaining the data is just one option for doing so. Microsoft, for instance, could order Dublin-based employees to collect the data and send it to the United States.

The Warrant allows any authorized law enforcement officer to search for and seize "[a]ll information . . . that constitutes fruits, evidence and instrumentalities" of certain crimes, including narcotics trafficking and money laundering. (*Id.* at Attach. C.) Regarding the place to be searched, the Warrant states, without any geographic limitation, that it "applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA 98052." (*Id.* at Attach. A.) While the Warrant lists the address of Microsoft's corporate headquarters, it purports to authorize the search of all "premises, owned, maintained, controlled, or operated by Microsoft" — anywhere in the world — where "information associated with" the subject email account may be found. (*Id.*) Microsoft currently manages more than one million server computers in datacenters worldwide, in more than 100 discrete leased and owned datacenter facilities, spread over 40 countries. (Decl. of Rajesh Jha, dated June 5, 2014, at ¶ 6 ("Jha Decl.").) These facilities host more than 200 online services, used by more than one billion customers and more than 20 million businesses worldwide. (*Id.*)

C. The Government Sought to Compel Microsoft to Search for and Seize User Content Located in Dublin on the Government's Behalf.

The Government served the Warrant on Microsoft and sought to compel Microsoft to assist in its execution, relying on 18 U.S.C. § 2703(a). Upon receipt of the Warrant, a Microsoft GCC team member in the United States determined that the content data associated with the targeted account is hosted in Microsoft's Dublin datacenter. (C.D. Decl., at ¶ 7.) Microsoft produced to the Government the non-content information and address book data that was located in the United States, but did not produce the user content located in Dublin. (*See* note 3, *supra*; C.D. Decl., at ¶ 8 & Ex. 2.)

D. Proceedings Before the Magistrate Judge

On December 18, 2013, Microsoft moved to vacate the Warrant to the extent it purported to authorize a search and seizure of content located in Ireland. (Mem. in Supp. of Mot. to Vacate, dated Dec. 18, 2013, Dkt. 6.) On April 25, 2014, the Magistrate Judge denied Microsoft's motion on the basis that the term "warrant" in section 2703(a) did not mean "warrant," but instead refers to a "hybrid: part search warrant and part subpoena." (Op. at 12, 23.) On May 5, the Magistrate Judge stayed his order pending appeal. (Dkt. 11.) On May 6, Microsoft appealed the Magistrate Judge's Order to this Court. (Dkt. 14.)[5]

III. Argument

A. Neither ECPA Nor Any Other Source of Law Authorizes The Court to Issue a Search Warrant for Information Stored Outside the United States.

1. ECPA and the Fourth Amendment Require the Government to Obtain a Warrant to Search and Seize the Contents of Email.

The Fourth Amendment protects the public's "papers and effects" from unreasonable searches and seizures. Courts have long held that this protection encompasses the content of communications, such as letters in the mail or telephone calls, in which individuals have a reasonable expectation of privacy. *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Katz v. United States*, 389 U.S. 347, 353 (1967).

---

[5] This Court reviews the Magistrate Judge's decision *de novo*. The Magistrate Judge's jurisdiction arose from the "catch-all provision" in 28 U.S.C. § 636(b)(3). This provision prescribes no standard of review, but "courts have borrowed . . . the dispositive-nondispositive distinction of subsection (b)(1)." *United States v. Warshay*, No. 98–CV–1245, 1998 WL 767138, at *3 (E.D.N.Y. Aug. 4, 1998); *see also Rajaratnam v. Moyer*, 47 F.3d 922, 924 n.8 (7th Cir. 1995). Under subsection (b)(1), a district court reviews *de novo* the dispositive ruling of a magistrate judge. 28 U.S.C. § 636(b)(1)(B)–(C). The Magistrate Judge's decision is dispositive because it resolved a motion "set[ting] forth all of the relief requested" by Microsoft. *ALCOA v. EPA*, 663 F.2d 499, 501 (4th Cir. 1981).

In 1986, with the advent of modern communications technologies such as email, Congress enacted ECPA, a statute intended to protect individuals' constitutionally-safeguarded expectations of privacy in electronic communications. *See* H.R. Rep. 99-647, at 22 (1986) ("Any discussion of the application of current law governing interception of e-mail or the use of e-mail surveillance begins with the Fourth Amendment, which protects our reasonable expectation of privacy"). To protect these vital privacy interests, ECPA requires federal, state, and local officers, when seeking specified categories of electronic communications data, to use one of three forms of process — each with its own powers and limitations.

At one end of the spectrum is the "warrant." ECPA permits the Government to act "only pursuant to a warrant" when it seeks the contents of email communications in electronic storage for less than 180 days, or email content of any age if notice is not first given to the accountholder. *See* 18 U.S.C. § 2703(a) ("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 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." (emphasis added)); *id.* at § 2703(b).[6]

The Sixth Circuit, in a leading decision, held that the Fourth Amendment requires the Government to obtain a warrant in order to obtain the contents of all emails, including those older than 180 days. *See Warshak*, 631 F.3d at 288 ("[T]o the extent that [ECPA] purports to permit the government to obtain . . . emails warrantlessly, the [statute] is unconstitutional."). Reasoning

[6] Because this Warrant seeks "[t]he contents of *all* e-mails stored in the account," without regard to the age of the emails, there can be no dispute that ECPA's warrant requirement applies. (*See* Warrant, Attach. C (emphasis added).)

that "an email is analogous to a letter or a phone call," the court noted that "the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call — unless they get a warrant, that is." *Id.* at 286. The court concluded that "if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception." *Id.* The Government has not contested *Warshak* and has followed its requirements.[7]

At the other end of the ECPA spectrum are subpoenas, 18 U.S.C. § 2703(b)(1)(B)(i), which may be used to obtain different categories of user information (but not content less than 180 days old). *See* 18 U.S.C. § 2703(a). "Congress legislates against the backdrop of existing law," *McQuiggin v. Perkins*, 133 S. Ct. 1924, 1934 n.3 (2013), so it is presumed to have understood that subpoenas and warrants are fundamentally distinct forms of process. A warrant constitutes the judicial authorization, founded on a finding of probable cause, of an activity that is uniquely assigned to law enforcement: the forcible entry into private property for the purposes of conducting a search and seizure. *See* BLACK'S LAW DICTIONARY 1470 (9th ed. 2009) (a warrant is "[a] judge's written order authorizing a law-enforcement officer to conduct a search of a specified place and to seize evidence"); *see also United States v. Kyles*, 40 F.3d 519, 523–24 (2d Cir. 1994). This power includes, for example, the right to "break open any outer or inner door or window" if the officer "is refused admittance." 18 U.S.C. § 3109. A search warrant is directed

---

[7] *See* Decl. of Claire Catalano ("Catalano Decl."), Ex. 1 (Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union (April 19, 2013) (confirming that the United States Attorney's Office for the Southern District of New York has not, since *Warshak*, "authorized a request to a court for access to the contents of a person's private electronic communications for law enforcement purposes without a warrant or on a standard less than probable cause")).

toward a place to be searched, rather than at a person who might possess or control the sought-after evidence, and by its nature provides no opportunity for notice or opportunity to object. *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000).

Subpoenas, in contrast, "command a person to appear before a court," for example "to bring specified documents, records, or things." BLACK'S LAW DICTIONARY 1563 (9th ed. 2009); Fed. R. Crim. P. 17(c)(1) ("[a] subpoena may order the witness to produce any books, papers, documents, data, or other objects"). Unlike warrants, they do not authorize "searches" and are thus not directed at particular locations. Rather, they can require recipients to collect and produce materials in their possession, custody, or control, wherever the location. *See United States v. King*, No. 94-CR-455, 1997 WL 582882, at *2 (S.D.N.Y. Sept. 19, 1997). And, whereas "the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues," a "subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded." *In re Subpoena Duces Tecum*, 228 F.3d at 348.

These fundamental distinctions between warrants and subpoenas are embodied in ECPA. Warrants under ECPA, like all warrants, require the Government to establish probable cause, but once issued by the court, may be executed without notice to the user, and *must* be issued by a magistrate judge once the required cause is shown. Fed. R. Crim. P. 41(d)(1). Unlike warrants, subpoenas issued under ECPA must be accompanied by notice to the user (with statutorily specified exceptions), *see* 18 U.S.C. §§ 2703(b)(1)(B)(i); 2705(a)(1)(B), and are enforced at the court's discretion, *see* Fed. R. Crim P. 17(c). This notice affords targets of a subpoena issued under ECPA the same opportunity for *ex ante* challenge they have outside the ECPA context.

That discretion allows a court to consider other factors (such as international comity) that weigh against enforcing a subpoena.[8]

2. The Term "Warrant" in ECPA Must Be Given its Ordinary Meaning, Including Attendant Limitations.

Given ECPA's plain language and structure (as well as its legislative history), it is clear that when Congress used the term "warrant" in 18 U.S.C. §2703(a), it meant "warrant" — with all of its attendant powers and limitations. As noted, *supra*, note 8, Congress, in fact, created a third type of process in ECPA — a "Court Order" issued under 18 U.S.C. § 2703(d) — which it required the Government to use to collect certain types of information. But, in addressing the production of the contents of recent emails — a person's most sensitive information — Congress declined to use a "hybrid" instrument or court order, but rather insisted on a warrant. *See* 18 U.S.C. § 2703(a), (b). The statute thus incorporates by reference an existing form of legal process — a warrant — with an established meaning, including well-understood powers and limitations.

Courts must "respect Congress' decision to use different terms to describe different categories of people or things." *Mohamad v. Palestinian Authority*, 132 S. Ct. 1702, 1708 (2012). Here, Congress understood the distinctions between warrants and subpoenas and intended for them to be treated differently under ECPA. *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),

---

[8] On the ECPA spectrum between warrants and subpoenas are court orders issued under 18 U.S.C. § 2703(d). Such orders allow the Government to obtain more user information than with a subpoena (but still not content less than 180 days old), on less than a showing of probable cause, and may be issued in the discretion of the court. *See In re Application of the United States*, 620 F.3d 304, 315–19 (3d Cir. 2010). Unlike warrants and subpoenas — established forms of process that pre-existed ECPA — § 2703(d) orders are an innovation of ECPA.

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)).

The legislative history of ECPA confirms that when Congress used the term "warrant," it intended to incorporate the pre-existing form of legal process. ECPA's warrant requirement resulted from Congress's recognition that "[a]dditional legal protection [for electronic communications] is necessary to ensure the continued vitality of the Fourth Amendment." H.R. Rep. 99-647 at 19. The drafters of ECPA correctly predicted that courts would hold that "parties to an e-mail transmission have a 'reasonable expectation of privacy'" and "enjoy a higher degree of Fourth Amendment protection." *Id.* at 22–23. Congress analogized digital customer content to the contents of safety deposit boxes, *id.* at 23 n.41, telephone calls, and regular mail, *see* S. Rep. 99-541, at 5 (1986). and sought to replicate to the contents of electronic communications the constitutional protections applicable to more traditional "papers and effects."

Moreover, when ECPA was enacted in 1986, the statute required that communications providers disclose content "only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant." Pub. L. No. 99-508 § 201, 100 Stat. 1861 (1986). That is, the statute required a traditional warrant, issued pursuant to Rule 41, in all cases. Congress amended this language in 2001 to require that such a warrant be "issued using the procedures described in the Federal Rules of Criminal Procedure . . . *by a court of competent jurisdiction*." 18 U.S.C. § 2703(a) (emphasis added). The legislative history of this amendment makes clear that the change did "*not affect the requirement for a search warrant*." H.R. Rep. No. 107-236, at 57 (2001) (emphasis in original). Instead, it allowed "a single court having jurisdiction over the offense to issue a search warrant for email that would be valid in [sic] anywhere in the

United States," which otherwise would be contrary to Rule 41. *See* 147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001).[9]

Like all warrants, warrants executed pursuant to ECPA must comply with constitutional requirements. *See United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011) (applying Fourth Amendment standards in assessing the validity of an ECPA warrant). One of those limitations is the Fourth Amendment's requirement that "no Warrants shall issue, [without] . . . particularly describing the place to be searched, and the persons or things to be seized." The particularity requirement applies no less to warrants issued under ECPA than it does to warrants for the search of a house or an office. *See id.*; *see also* Fed. R. Civ. P. 41(e)(2)(A) ("the warrant must identify the . . . *property* to be searched [and] identify any . . . *property* to be seized"); *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) ("[T]he procedures for issuing a warrant are enumerated at Rule 41(e), which of course, would apply to § 2703(a).").

The Government takes the extraordinary position that warrants issued under ECPA involve no constitutional "search" at all. (*See* Transcript of Oral Argument, Mar. 21, 2014, at 25:4–9.) Not only does this position ignore the face of the "Search and Seizure Warrant" issued here, it contradicts the legislative history of ECPA and *Warshak*, which both recognize that email

---

[9] The amendment was intended to help law enforcement respond more quickly to potential threats by allowing officers to obtain warrants from a single judicial district that could be executed nationwide, instead of requiring them to obtain a warrant from each judicial district in which electronic evidence was located. H.R. Rep. 107-236, at 57 (2001). Prior to this change an investigator "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 a warrant to search." H.R. Rep. 107-236, at 57 (2001). In context, it is clear that Congress discussed "where the ISP is located" because it assumed that was the same place as where the "Internet service provider (ISP) account [was] located"; the Magistrate Judge misread this legislative history in suggesting that statute focuses on the location of the ISP, rather than the data to be searched and seized. (Op. at 17.)

communications are entitled to a reasonable expectation of privacy. Government infringement of that expectation is the very definition of a "search." *Warshak*, 631 F.3d at 286–88.

Moreover, in the context of electronic data, the "place to be searched" is the physical location where the data is stored. In *United States v. Gorshkov*, for example, federal agents seized a computer in the United States and used it to access data stored in Russia. No. CR00-550C, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001). The court concluded that the "extraterritorial access to computers in Russia" constituted a "search or seizure of . . . property outside the territory of the United States." *Id.* at *3. Similarly, in *In re Warrant to Search a Target Computer at Premises Unknown*, the court rejected the Government's application for a search warrant because the location of the target computer was unknown and it was the location of the computer (and the data on it) that determined where the search took place. No. H-13-234M, 2013 WL 1729765, at *3 (S.D. Tex. Apr. 22, 2013). These cases are consistent with Rule 41, which emphasizes the location of the data in prescribing the procedures for warrants. *See* Rule 41(e)(2)(B) (addressing "electronically stored information" and drawing a distinction between the "seizure or *on-site* copying of the media or information" and the "later *off-site* copying or review" (emphases added)).[10]

3. ECPA Warrants, Like All Warrants, Are Confined to the Territory of the United States.

[10] Warrants for remotely stored electronic data also involve the *seizure* of that data at the place where it is stored. Copying an individual's private computer data constitutes a seizure because creation of a copy deprives the individual of "exclusive rights to the data." *Matter of Search of Information Associated with [Redacted]@mac.com*, --- F. Supp. 2d. ----, 2014 WL 1377793, at *3 (D.D.C. 2014) (quoting Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 703 (2010) ("Kerr, *Seizures of Computer Data*")); *see also* Kerr, *Seizures of Computer Data* at 721–22 (concluding that seizure occurs when a person's private data is copied "outside the intended scope of transmission or use").

It is well established, and there was no dispute below, that courts in the United States lack authority to issue warrants for extraterritorial searches and seizures. *See United States v. Vilar*, No. 05-CR-621, 2007 WL 1075041, at *52 (S.D.N.Y. Apr. 4, 2007) ("[T]here 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"). The Second Circuit has expressly confirmed the absence of any authority to issue such extraterritorial warrants. *See United States v. Odeh*, 552 F.3d 157, 169 (2d Cir. 2008) ("[S]even 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."). And the Supreme Court has explicitly rejected a proposed amendment to Rule 41 that would have permitted the issuance of warrants authorizing searches and seizures of property outside of the United States. *See* Fed. R. Crim. P. 41, Notes of Advisory Committee on Rules — 1990 Amendment.[11]

---

[11] Rule 41 demonstrates that the Supreme Court and Congress recognize the territorial limits of the warrant power. By its terms, Rule 41 provides that warrants may be issued for searches outside of U.S. borders — but still on territory subject to U.S. jurisdiction — in three limited circumstances: (A) for searches conducted in a United States territory, possession, or commonwealth; (B) for searches of the premises of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or (C) for searches of a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state. *See* Fed. R. Crim. P. 41(b)(5). While we acknowledge that Judge Kaplan has questioned whether Rule 41(b) applies to warrants served pursuant to section 2703(a), *see Hubbard v. Myspace, Inc.*, 788 F. Supp. 2d 319, 325 n.18 (S.D.N.Y. 2011), there is no question that, at a minimum, Rule 41(b) demonstrates that the Supreme Court and Congress know how to confer expressly the authority to execute warranted searches outside of U.S. borders when they wish to do so.

Even if Congress could constitutionally empower courts to issue extraterritorial warrants, nothing in the text or legislative history of ECPA suggests that Congress intended to vest courts with such authority when it authorized the Government to compel providers to assist in the execution of warrants for stored email content. To the contrary, the legislative history of ECPA confirms that warrants executed pursuant to 18 U.S.C. § 2703(a) are limited to the territory of the United States. In 2001, Congress amended ECPA to provide that warrants could be issued by a magistrate judge with jurisdiction over the offense under investigation, even for electronic data located outside the magistrate judge's district. The very title of the amendment, however, made clear that the authorization did not extend beyond the territory of the United States. *See* Pub. L. No. 107-56 § 220, 115 Stat. 291 (2001) (entitled "*Nationwide* Service of Search Warrants for Electronic Evidence." (emphasis added)). The legislative history further demonstrates that the intent of the amendment was to allow magistrate judges to issue warrants to be executed outside of their home districts — but still inside the United States. 147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) (amendment would "[p]ermit[] 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*." (emphasis added)). As *Vilar* recognized, "nothing in the language of [the 2001 ECPA] amendment remotely suggests that the power [of a magistrate to authorize a search of his or her district] extended to extraterritorial searches." 2007 WL 1075041, at *52 n.33.

4. Interpreting ECPA to Authorize Searches and Seizures Outside the United States Would Violate International Law And Raise Serious Foreign Policy Concerns That Congress Presumptively Would Have Sought to Avoid.

ECPA's plain language and legislative history establish that warrants served on providers under the statute, like ordinary warrants, cannot validly authorize extraterritorial searches and seizures. This interpretation is reinforced by the serious adverse foreign policy consequences

that would follow if ECPA were interpreted to authorize the search and seizure of data stored in another sovereign country. Such an expansive reading would violate two well-established canons of statutory construction:

Presumption against extraterritoriality. It is settled that "[w]hen a statute gives no *clear* indication of an extraterritorial application, it has none." *Morrison*, 130 S. Ct. at 2878 (emphasis added). This presumption against extraterritoriality "serves to protect against unintended clashes between our laws and those of other nations which could result in international discord." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013). In other words, it reflects the fact "that United States law governs domestically but does not rule the world." *Id.* Section 2703(a) contains no indication — let alone the required "clear indication" — that Congress intended to vest courts with the authority to issue extraterritorial warrants. To the contrary, the legislative history of the statute makes clear that it was intended to have effect *only* "anywhere *in the United States*." 147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) (emphasis added); *see also Zheng v. Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297, at *4 (N.D. Cal. Dec. 2, 2009) (applying the presumption against extraterritoriality to ECPA).

Charming Betsy. Interpreting ECPA to authorize extraterritorial searches would violate the equally fundamental precept that to the maximum possible extent statutes should be interpreted consistent with international law. "It has been a maxim of statutory construction since the decision in *Murray v. The Charming Betsy*, that an act of congress ought never to be construed to violate the law of nations, if any other possible construction remains." *Weinberger*, 456 U.S. at 32 (citation and quotation marks omitted). Applying the *Charming Betsy* doctrine, the Supreme Court requires "some affirmative expression of congressional intent to abrogate the United States' international obligations" before construing a statute to do so. *Id.* at 33.

The Government's interpretation of ECPA would violate international law (and thereby run contrary to the *Charming Betsy* canon) in at least two ways. First, it is a bedrock principle of international law that "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state." RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 432(2); *see also United States v. Blanco*, 861 F.2d 773, 779 (2d Cir. 1988) ("The United States has no right to enforce its laws in another country without that country's consent or acquiescence." (citing the Restatement)). Reaching across international borders to obtain data from foreign servers without the foreign sovereign's permission would lead to serious international friction; "it takes little to imagine the diplomatic and legal complications that would arise if American government officials traveled to another sovereign country and attempted to carry out a search of any kind, professing the authority to do so based on an American-issued search warrant." *Odeh*, 552 F.3d at 171 (internal quotation marks omitted).[12]

Second, the Government's interpretation of ECPA would infringe the U.S.'s obligation to perform its treaty commitments in good faith. *See* Vienna Convention on the Law of Treaties art. 27, May 22, 1969 (a "treaty in force is binding . . . and must be performed . . . *in good faith*."). Here, the United States has entered into MLATs with Ireland and the European Union that establish procedures — including expedited procedures — by which the United States may obtain data stored in Ireland. *See* Mutual Legal Assistance Treaty Between the United States of America and Ireland ("Irish-US MLAT"), art. 14, T.I.A.S. 13137, Jan. 18, 2001 (search and sei-

[12] And it is not just federal law enforcement that could reach across national boundaries to execute searches and seizures under the Government's interpretation of ECPA. ECPA explicitly contemplates warrants obtained by state and local law enforcement agencies as well. *See* 18 U.S.C. §§ 2703(a), 2711(3)(B). There is no reason to think Congress silently empowered individual state and local law enforcement officers and state courts to determine for themselves when and whether to intrude upon a foreign nation's sovereignty by seeking warrants to conduct searches in that sovereign's territory without its permission.

zure requests); Agreement on Mutual Legal Assistance Between the European Union and the United States of America ("EU-US MLAT"), arts. 3 & 7, June 25, 2003, T.I.A.S. 10-201.1 (applying EU-US MLAT to MLATs already in force between US and EU member states). While Congress may abrogate such treaty obligations, "unless this power is clearly and unequivocally exercised, th[e] court is under a duty to interpret statutes in a manner consonant with existing treaty obligations." *United States v. Palestine Liberation Org.*, 695 F. Supp. 1456, 1465 (S.D.N.Y. 1988). The Magistrate Judge's ruling violates this principle by allowing the Government to end run the MLATs that the United States has signed with Ireland and the EU.

5. The Warrant Purports to Conscript Microsoft to Execute an Invalid Extraterritorial Search and Seizure on the Government's Behalf.

The Government has conscripted Microsoft to assist in the execution of the Warrant, but that does not make the search and seizure any less extraterritorial or otherwise cure this fundamental flaw. The Warrant commands the *Government* to enter Microsoft's premises — by force, if necessary — and seize the relevant customer information. The Warrant is directed "To: Any authorized law enforcement officer" and states "YOU ARE COMMANDED to execute this warrant . . . in the daytime 6:00 a.m. to 10:00 p.m." (Warrant, at 2.) But, just as the Government is unable to undertake such a foreign search and seizure *directly*, it may not seek to execute the Warrant *indirectly* by conscripting Microsoft to act in its stead. *See Skinner v. Ry. Labor Execs' Ass'n*, 489 U.S. 602, 614 (1989) (when a company executes a search "by compulsion of sovereign authority," it "act[s] as an instrument or agent of the Government" and its conduct "is controlled by the Fourth Amendment"). Since the Government cannot conduct a warranted search outside the United States, Microsoft — the Government's "instrument" — cannot either.

Nor is there any question that the Government sought through the Warrant to conduct an extraterritorial search and seizure. The Government has directed Microsoft to conduct a search

of Microsoft's own servers for the targeted email account data, seize that data, and disclose it to the Government. This search-and-seizure — undertaken by Microsoft as the conscripted agent of the Government — would take place in Ireland.

6. The Magistrate Judge Erred by Concluding That Congress Intended Warrants Issued Under ECPA to Have Global Reach.

In his Order, the Magistrate Judge accepted that courts generally lack authority to issue extraterritorial warrants (Op. at 22–23), but concluded that this long-standing rule applies only to "conventional warrants," not warrants executed pursuant to ECPA. (*Id.*) In the Magistrate Judge's view, a warrant served on a provider under ECPA is a "hybrid: part search warrant and part subpoena." (*Id.* at 23.) The Magistrate Judge then concluded that since *subpoenas* can compel a recipient to produce data stored outside the United States, so too can a warrant served on a provider under ECPA. (*Id.*)

This interpretation violates the most basic rule of statutory construction that words in a statute should be afforded their ordinary meaning. *See Milner v. Dep't of Navy*, 131 S. Ct. 1259, 1264 (2011). As discussed above, the term "warrant" has a well-established meaning, and it is not the "hybrid" meaning the Magistrate Judge devises. By conflating warrants and subpoenas into a hybrid "SCA Warrant" (Op. at 8), the Magistrate Judge disregarded the fundamental differences between them — differences that are highlighted by the fact that ECPA expressly incorporates warrants, subpoenas, and court orders, and assigns different roles to each.[13]

---

[13] The Magistrate Judge also distinguished this Warrant from "conventional warrants" on the ground that the requirement stems solely from ECPA and not the Constitution. (Op. at 23.) This holding ignores both *Warshak* and ECPA's legislative history, which make clear that emails are protected from unreasonable searches and seizures by the Fourth Amendment. Moreover, we have located no case in which a U.S. company has been required by subpoena to search for and seize the private "papers and effects" of a third party. Indeed, the case law is clear that subpoenas cannot compel businesses to search for and seize constitutionally-protected property belonging to their customers. Thus, a mail carrier cannot be forced to "invade the secrecy of letters and (continued...)

In concluding that warrants executed under ECPA are "part search warrant and part subpoena," the Magistrate Judge focused on the fact that section 2703(a) does not refer to warrants issued "pursuant to the Federal Rules of Criminal Procedure," but rather to "warrants" "*issued using the procedures described in the Federal Rules of Criminal Procedure*." (Op. at 10.) According to the Magistrate Judge, this language is ambiguous because it could either mean (i) "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"; *or* (ii) "while procedural aspects of the application process are to be drawn from Rule 41 . . . more substantive rules are derived from other sources" — *i.e.*, the law governing subpoenas. *Id.*

But there is no ambiguity, and even if there were, it would not support the Magistrate Judge's conclusion. First, regardless of whether "the procedures described in the Federal Rules of Criminal Procedure" — as that phrase is used in ECPA — incorporates Rule 41(b)'s limitation to domestic searches (with three narrow exceptions), there can be no dispute that those "procedures" *do* include Rule 41(e), *see Berkos*, 543 F.3d at 397–98, which establishes electronic data is located physically where it is "on site"— here, Dublin, Ireland. Second, Congress used the term "warrant." A territorial limitation on courts' power to issue warrants need not be stated expressly; it is the default rule, reinforced by the presumption against extraterritoriality and the

---

such sealed packages in the mail" absent a valid warrant. *See United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) (quoting *Ex parte* Jackson, 96 U.S. 727, 733 (1878)). And while a subpoena may compel a bank to turn over records it maintains about customers, the Government must obtain a warrant to search for evidence in a customer's safe deposit box at the bank. *See, e.g., United States v. Thomas*, 878 F.2d 383, at *2 (6th Cir. 1989) (per curiam). The legislative history of ECPA reflects this distinction. *See* H.R. Rep. 99-647 at 23 n.41 (stating that "contents of customer data enjoy a higher degree of Fourth Amendment protection" than non-content, and noting that "[u]nlike records of the bank's . . . , contents are analogous to items stored, under the customer's control, in a safety deposit box"). By conflating warrants with subpoenas, the Magistrate Judge's ruling ignores these limits.

Charming Betsy canon. In the *absence* of *any* source of law that expressly permits courts to authorize extraterritorial searches and seizures, they may not. *See Odeh*, 552 F.3d at 169–71. And ECPA did not expressly grant courts the power to issue extraterritorial warrants.

Having incorrectly conflated warrants and subpoenas, the Magistrate Judge concluded that the resulting "hybrid" instrument can compel Microsoft "to produce information . . . regardless of the location of that information." (Op. at 13.) The Magistrate Judge relied for this proposition on a line of cases, often referred to as the *Bank of Nova Scotia* (or *"BNS"*) doctrine, that stand for the proposition that a party subject to U.S. jurisdiction can be compelled by grand jury subpoena to produce evidence stored outside the United States so long as the evidence is within the party's "possession, custody, or control." *See id.* (citing, *inter alia*, *Marc Rich & Co. v. United States*, 707 F.2d 663, 670 (2d Cir. 1983)). The *BNS* doctrine, however, has never been applied to a search warrant, and with good reason. A subpoena focuses on the *person* with possession, custody, or control over the evidence, whereas a warrant is directed to the evidence itself and its location. *Compare Marc Rich & Co.*, 707 F.2d at 667 (noting that the recipient of a subpoena is compelled as a matter of "public duty" to collect and produce the responsive evidence) *with* Fed. R. Civ. P. 41(e)(2)(A) ("the warrant must identify the . . . *property* to be searched [and] identify any . . . *property* to be seized." (emphasis added)).[14]

Setting aside the inapplicability of *BNS* to warrants, the Magistrate Judge's decision would also vitiate an integral part of the *BNS* doctrine: the opportunity for *ex ante* review on

---

[14] The *BNS* doctrine is inapposite to ECPA warrants for a second, distinct reason: it focuses on the production of a corporate entity's business records, not on personal communications held by a provider on behalf of a customer. In *Marc Rich & Co.*, for example, the grand jury subpoena sought the recipient's "business records relating to crude oil transactions during 1980 and 1981." 707 F.2d at 665. Here, by comparison, the Warrant does not seek *Microsoft's* business records, but rather substantive communications of *Microsoft's customer*.

comity grounds. *See United States v. Davis*, 767 F.2d 1025, 1033–34 (2d Cir. 1985) (adopting a multi-factor analysis set out in the Restatement of Foreign Relations Law "in evaluating the propriety of a subpoena directing the production of information or documents located abroad when such production would violate the law of the state in which the documents are located"). One of the factors set out in *Davis* is "the possibility of alternative means of securing the information," — *e.g.*, through an MLAT. *Id.* at 1034 n.16. This *ex ante* review is possible for subpoenas issued under ECPA, because, as discussed above, subpoenas are generally accompanied by notice to the subscriber. If the Government seizes data using a *warrant*, on the other hand, the Government is not required to notify the user, and the user, in turn, is unable to challenge the seizure *ex ante* on comity grounds. In applying *Bank of Nova Scotia* to warrants, in other words, the Magistrate Judge neglected the international comity analysis that is an integral part of the *BNS* doctrine.[15] It cannot be that an act that is *more* intrusive on a foreign sovereign — the execution of a warranted search by law enforcement authorities of another country — is afforded *less* consideration of international comity concerns.

Finally, the Magistrate Judge erred in his conclusion that the Warrant does "not implicate principles of extraterritoriality" (Op. at 12), because, in his view, this case "does not involve the deployment of American law enforcement personnel abroad" and "places obligations only on the service provider to act within the United States" (Op. at 21–22). This conclusion is wrong on both counts. First, while the Government may not contemplate the deployment of federal agents to Ireland in this case, that is only because the Government has chosen to conscript Microsoft to

[15] It is an open question whether the *BNS* doctrine remains good law — even in the context of grand jury subpoenas — following the Supreme Court's reinforcement of the presumption against extraterritoriality in *Morrison* and *Kiobel*. Even if the *BNS* doctrine survives *Morrison* and *Kiobel*, however, it does not apply to warrants.

execute this Warrant on its behalf. *See Skinner*, 489 U.S. at 614 (when a company executes a search "by compulsion of sovereign authority," it "act[s] as an instrument or agent of the Government" and its conduct "is controlled by the Fourth Amendment"). Second, the Warrant unequivocally *does* impose obligations on Microsoft, as the Government's conscript, to act outside the United States. [redacted] (*See* C.D. Decl., at ¶ 6.) In other words, both the search and the seizure of the relevant data would take place in Ireland. *See* note 4, *supra*.

B. Even if Permitted by ECPA, the Warrant Is Unlawful Because It Violates the Particularity Requirement of the Fourth Amendment to the Constitution.

Even if the Warrant at issue were permitted by statute, the Court should nevertheless vacate it as unconstitutional. The Fourth Amendment requires that all warrants specify with particularity the place to be searched and the things to be seized. The Warrant does not meet this requirement; to the contrary, it exemplifies the very form of governmental abuse the Fourth Amendment was intended to prohibit.

Courts have vigorously enforced this requirement, recognizing that failure to do so "would undermine the warrant requirement itself, and increase the risk of an excessive intrusion into the areas of personal rights protected by the Fourth Amendment." *United States v. Wuagneux*, 683 F.2d 1343, 1348–49 (11th Cir. 1982). These protections have not deteriorated as technology has advanced over time. *See Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

The Warrant here identifies the place to be searched as "premises, owned, maintained, controlled, or operated by Microsoft Corporation." (Warrant, Attach. A.) It does not limit the

Government's search to any specific facility or physical premises, but instead extends it to all digital information within Microsoft's possession *anywhere in the world*. This broadly-worded authorization plainly disregards the Fourth Amendment's particularity requirement. Rather than describe a "definitely ascertainable place so as to exclude all others," as the particularity requirement demands, *United States v. Lemmons*, 527 F.2d 662, 666 (6th Cir. 1975), the Warrant authorizes the search of any and all of Microsoft's offices, stores, and datacenters worldwide. To enforce a warrant of such indefinite boundaries would "condon[e] the use of the pernicious general warrant, and redact[] the particularity requirement from the fourth amendment." *United States v. Nafzger*, 965 F.2d 213, 216 (7th Cir. 1992). And, because the Warrant fails to state with particularity the "place to be searched," it also cannot possibly be supported by probable cause. *See United States v. Clark*, 638 F.3d 89 (2d Cir. 2011) ("[T]he confluence of the Fourth Amendment's probable cause and particularity requirements . . . demand that a search warrant for a multi-occupancy building be supported by a showing of probable cause as to each unit.").[16]

The Court should "construe the statute to avoid such [constitutional] problems" by giving the word "warrant," as used in ECPA, its ordinary meaning, and thus hold that the Warrant here cannot authorize the extraterritorial search and seizure sought by the Government. *United States v. Magassouba*, 544 F.3d 387, 404 (2d Cir. 2008).

C. The Government Should Seek the Relevant User Information by Following the Process Established by the US-Ireland MLAT.

The Magistrate Judge ultimately rested his decision on a practical concern that criminal investigations would be hampered "[i]f the territorial restrictions on conventional warrants ap-

---

[16] These constitutional defects cannot be cured. A more particular statement of the "place to be searched" would necessarily identify Microsoft's datacenter in Ireland, and the Warrant's improper extraterritoriality — and thus its invalidity — would be evident on its face.

plied to warrants issued under section 2703(a)." (Op. at 18.) But this was precisely the choice that Congress made when it enacted ECPA to protect the privacy of email users, and relied on the pre-existing warrant authority to do so. The Magistrate Judge erred in deferring to practical concerns as a basis for departing from the plain text of the statute.

If practical concerns are to be considered, however, the Court should consider *all* relevant circumstances. The Magistrate Judge dismissed the MLAT process as "slow and laborious" based on pure speculation. He relied on a single citation to a law review article (Op. at 19); the Government introduced no evidence to suggest that the MLAT process is inefficient.

To the contrary, as Michael McDowell, former Minister of Justice and Attorney General of Ireland, explains, Ireland has implemented its MLAT obligations with "highly effective" legislation that is "efficient and well-functioning." (Decl. of Michael McDowell, dated June 5, 2014 ("McDowell Decl."), at ¶ 8.) The MLATs create well-defined procedures to obtain the precise type of private email communications at issue here, in a manner that protects privacy interests, law enforcement objectives, and the territorial sovereignty of all parties. Ireland and the United States entered into their MLAT in 2001, more than a decade after ECPA was enacted and at a time when electronically-stored evidence was already a common feature of transnational criminal investigations. To the extent the Government needs such evidence urgently, there are procedures for expedited requests. *See* EU-US MLAT, art 7. For instance, when Irish authorities serve MLAT requests on Microsoft's compliance team in Dublin, Microsoft routinely responds within seven days. ([redacted] Decl., at ¶ 6.)[17]

---

[17] The Magistrate Judge's dim view of the MLAT is particularly unjustified in light of the close working relationship between the United States and Ireland. As Mr. McDowell explains, "[r]efusal by Ireland to execute a proper request duly made for assistance from U.S. authorities is very uncommon." (McDowell Decl., at ¶ 4); *see also* Law Enforcement Treaties: Hearing Before (continued...)

The Magistrate Judge's decision also stands to damage U.S. foreign relations. If sustained, it will empower the Government to violate the territorial sovereignty of another nation every time it executes a warrant for data stored abroad (or compels a provider to do so on its behalf). This will undermine the Government's ability to cooperate with other governments under established MLATs and imperil the negotiation of new MLATs in the future. Moreover, the Government's position could encourage foreign governments to side-step their own MLAT commitments and unilaterally seek data stored in the United States from providers that operate on their soil. Indeed, Brazil has recently enacted such legislation.[18] As foreign countries increasingly assert unilateral jurisdiction over data stored in the United States, the primary objective of ECPA — protecting citizens' most private electronic information — will be thwarted.

Finally, the Government's unilateral exercise of law enforcement powers within the territory of Ireland puts at risk the U.S. information technology sector's continued ability to compete globally. Within days of the Magistrate Judge's order in this case, foreign leaders expressed concern about the Magistrate Judge's expansive interpretation of ECPA, and noted that compliance with extraterritorial U.S. search warrants may cause providers to violate the data protection laws of the countries where the targeted data is stored.[19] These statements echoed earlier con-

---

the Committee on Foreign Relations of the U.S. Senate, 107th Cong. 19 (2002) (written statement of U.S. Department of State) ("On mutual assistance requests, Irish police cooperate extensively with U.S. law enforcement agents . . . ."). And if the Government is dissatisfied with the efficiency of Ireland's (or its own) compliance with the MLAT, it is readily capable of proposing amendments to it, or making operational improvements.

[18] *See* Catalano Decl., Ex. 2 (*How Brazil and the EU Are Breaking the Internet*, FORBES (May 19, 2014) (noting that new Brazilian Internet legislation enacted on April 24, 2014 "explicitly applies to any company anywhere that has at least one Brazilian user, has servers located in Brazil, or operates an office there, or effectively, all Internet companies on Earth.")).

[19] *See* Catalano Decl., Ex. 3 (Letter from Sophie in't Veld, Member of the European Parliament, to Viviane Reding, Vice-President of the European Commission (April 28, 2014)); *id* at Ex. 4 (*Microsoft 'must release' data held on Dublin server*, BRITISH BROAD. CORP. (April 29, (continued...)

cerns voiced by the European Commission that "[i]f U.S. authorities circumvent the Mutual Legal Assistance agreement and access data directly (through companies) for criminal investigations, they expose companies operating on both sides of the Atlantic to significant legal risks." (*See* Decl. of Claire Catalano, Ex. 5 (European Commission, *Restoring Trust in EU-US data flows* – Frequently Asked Questions (Nov. 27, 2013) (noting that "[a] solution would be for U.S. law enforcement authorities to use formal channels, such as the MLA, when they request access to personal data located in the EU and held by private companies").)

Microsoft also has encountered rising concerns among both current and potential customers overseas about the U.S. Government's extraterritorial access to their user information. (Jha Decl., at ¶ 8.) In some instances, potential customers have decided not to purchase services from Microsoft and have opted instead for a provider based outside the United States that is perceived as being not subject to U.S. jurisdiction. (*Id.* at ¶ 9.) Some of these customers have specifically referred to the decision below as a basis for concern about U.S. Government access to customer data. (*Id.* at ¶ 10). If this trend continues, the U.S. technology sector's business model of providing "cloud" Internet-based services to enterprises, governments, and educational institutions worldwide will be substantially undermined. (*Id.* at ¶ 12.)

IV. Conclusion

For the foregoing reasons, the Court should reverse the Magistrate's Order and grant Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States.

2014) (quoting Mina Andreeva, European Commission spokeswoman for justice, fundamental rights and citizenship as stating "The commission's position is that this data should not be directly accessed by or transferred to US law enforcement authorities outside formal channels of cooperation, such as the mutual legal assistance agreements.")).

Dated: June 6, 2014

Respectfully submitted,

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

E. Joshua Rosenkranz
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Tel: 212.506.5380
jrosenkranz@orrick.com

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION

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

**Admitted pro hac vice*

Counsel for Microsoft Corporation