

# 14-2985

*To Be Argued By:*  
JUSTIN ANDERSON

---

United States Court of Appeals

**FOR THE SECOND CIRCUIT**

**Docket No. 14-2985**



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

MICROSOFT CORPORATION,

*Appellant,*

—v.—

UNITED STATES OF AMERICA,

*Appellee.*

ON APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK

---

---

**BRIEF FOR THE UNITED STATES OF AMERICA**

---

---

PREET BHARARA,  
*United States Attorney for the  
Southern District of New York,  
Attorney for the United States  
of America.*

JUSTIN ANDERSON,  
SERRIN TURNER,  
*Assistant United States Attorneys,  
Of Counsel.*

---

---

**TABLE OF CONTENTS**

	PAGE
Preliminary Statement . . . . .	1
Statement of Facts . . . . .	2
A. The Warrant Served on Microsoft . . . . .	2
B. The Proceedings Before the Magistrate Judge . . . . .	5
C. The Proceedings Before the Chief District Judge . . . . .	7

ARGUMENT:

The SCA Authorizes the Use of Warrants to Compel the Production of Records Regardless of Where They Are Stored. . . . .	8
A. Applicable Law . . . . .	10
1. The Stored Communications Act . . . . .	10
2. The Compelled Production of Records Stored Abroad . . . . .	14
B. Discussion . . . . .	17
1. The SCA Requires the Disclosure of Records by Warrant. . . . .	17
2. Nothing in the SCA’s Text, Structure, Purpose, or Legislative History Indicates that Compelled Production of Records Is Limited to Those Stored Domestically. . . . .	26

	PAGE
3. Compliance with the Warrant Does Not Implicate the Presumption Against Extraterritoriality . . . . .	31
4. The Warrant Can Compel Microsoft to Produce Emails in the Account Regardless of Who “Owns” Them . . . .	36
5. Compliance with the Warrant Does Not Implicate Any Genuine Conflict of Laws That Would Raise Comity Concerns . . . . .	44
6. Policy Considerations Weigh Against Creating an Easily Abused Loophole in the SCA’s Comprehensive Disclosure Requirements . . . . .	48
CONCLUSION . . . . .	58

**TABLE OF AUTHORITIES**

*Cases:*

<i>Bay Ridge, Inc. v. Fed’l Mine Safety &amp; Health Review Comm’n</i> , 715 F.3d 631 (7th Cir. 2013). . . . .	21
<i>Blackmer v. United States</i> , 284 U.S. 421 (1932). . . . .	6, 14
<i>Cannon v. Univ. of Chicago</i> , 441 U.S. 677 (1979). . . . .	27

	PAGE
<i>Drescher v. Shatkin</i> , 280 F.3d 201 (2d Cir. 2002) . . . . .	18
<i>Duncan v. Belcher</i> , 813 F.2d 1335 (4th Cir. 1987) . . . . .	19
<i>Envtl. Def. Fund. v. Massey</i> , 986 F.2d 528 (D.C. Cir. 1993). . . . .	33
<i>First Nat. City Bank v. I.R.S.</i> , 271 F.2d 616 (2d Cir. 1959) . . . . .	15, 56
<i>Fisher v. United States</i> , 425 U.S. 391 (1976). . . . .	35
<i>Hale v. Henkel</i> , 201 U.S. 43 (1906). . . . .	15, 34
<i>In re Grand Jury Proceedings (Bank of Nova Scotia)</i> , 740 F.2d 817 (11th Cir. 1984) . . . . .	16, 26, 57
<i>In re Grand Jury Subpoena Dated August 9, 2000</i> , 218 F. Supp. 2d 544 (S.D.N.Y. 2002). . . . .	17
<i>In re Grand Jury Subpoena</i> , 646 F.3d 159 (4th Cir. 2011) . . . . .	49
<i>In re Grand Jury Subpoenas</i> , 318 F.3d 379 (2d Cir. 2003) . . . . .	52
<i>In re Horowitz</i> , 482 F.2d 72 (2d Cir. 1973) . . . . .	38
<i>In re Marc Rich &amp; Co.</i> , 707 F.2d 663 (2d Cir. 1983) . . . . .	<i>passim</i>
<i>In re Search</i> , 13 F. Supp. 3d 157 (D.D.C. 2014) . . . . .	34

	PAGE
<i>In re Warrant to Search a Certain E-Mail Account</i> , 15 F. Supp. 3d 466 (S.D.N.Y. 2014) . . . . .	<i>passim</i>
<i>Johnson v. United States</i> , 123 F.3d 700 (2d Cir. 1997) . . . . .	48
<i>Kaufman v. Edelstein</i> , 539 F.2d 811 (2d Cir. 1976) . . . . .	57
<i>Linde v. Arab Bank, PLC</i> , 706 F.3d 92 (2d Cir. 2013) . . . . .	14, 16
<i>Minnesota v. Carter</i> , 525 U.S. 83 (1998) . . . . .	43
<i>Morrison v. Nat’l Austl. Bank Ltd.</i> , 561 U.S. 247 (2010) . . . . .	31, 32, 33, 36
<i>Oklahoma Press Pub. Co. v. Walling</i> , 327 U.S. 186 (1946) . . . . .	34
<i>Ridge, Inc. v. Fed’l Mine Safety &amp; Health Review Comm’n</i> , 715 F.3d 631 (7th Cir. 2013) . . . . .	21
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014) . . . . .	55
<i>Skinner v. Railway Labor Executives Ass’n</i> , 489 U.S. 602 (1989) . . . . .	35
<i>Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court</i> , 482 U.S. 522 (1987) . . . . .	16, 49
<i>United States v. Alvarez-Machain</i> , 504 U.S. 655 (1992) . . . . .	49
<i>United States v. Bach</i> , 310 F.3d 1063 (8th Cir. 2002) . . . . .	23, 25

	PAGE
<i>United States v. Barr</i> , 605 F. Supp. 114 (S.D.N.Y. 1985) . . . . .	39
<i>United States v. Bausch &amp; Lomb Optical Co.</i> , 321 U.S. 707 (1944). . . . .	34
<i>United States v. Berkos</i> , 543 F.3d 392 (7th Cir. 2008) . . . . .	25
<i>United States v. Chase Manhattan Bank, N.A.</i> , 584 F. Supp. 1080 (S.D.N.Y. 1984) . . . . .	17, 26
<i>United States v. Davis</i> , 767 F.2d 1025 (2d Cir. 1985) . . . . .	44
<i>United States v. First Nat'l City Bank</i> , 379 U.S. 378 (1965). . . . .	32
<i>United States v. First National City Bank</i> , 568 F.2d 853 (2d Cir. 1977) . . . . .	39
<i>United States v. First Nat. City Bank</i> , 396 F.2d 897 (2d Cir. 1968) . . . . .	<i>passim</i>
<i>United States v. Ganas</i> , 755 F.3d 125 (2d Cir. 2014) . . . . .	35
<i>United States v. Giovanelli</i> , 747 F. Supp. 891 (S.D.N.Y. 1989) . . . . .	39
<i>United States v. Guterma</i> , 272 F.2d 344 (2d Cir. 1959) . . . . .	40, 41
<i>United States v. Punn</i> , 737 F.3d 1 (2d Cir. 2013) . . . . .	8
<i>United States v. Rommy</i> , 506 F.3d 108 (2d Cir. 2007) . . . . .	49

	PAGE
<i>United States v. Safavian</i> , 644 F. Supp. 2d 1 (D.D.C. 2009) . . . . .	52
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990). . . . .	44
<i>United States v. Vetco, Inc.</i> , 691 F.2d 1281 (9th Cir. 1981) . . . . .	17
<i>United States v. Vilar</i> , 729 F.3d 62 (2d Cir. 2013) . . . . .	32
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010) . . . . .	28, 43
<i>United States v. Wilkerson</i> , 361 F.3d 717 (2d Cir. 2004) . . . . .	36
<i>Warden v. Hayden</i> , 387 U.S. 294 (1967). . . . .	41
 <i>Statutes, Rules &amp; Other Authorities:</i>	
12 U.S.C. § 3402 . . . . .	19
12 U.S.C. § 3406 . . . . .	19
18 U.S.C. § 1030 . . . . .	50
18 U.S.C. § 2703 . . . . .	<i>passim</i>
18 U.S.C. § 2711 . . . . .	22, 30
18 U.S.C. § 3105 . . . . .	23
18 U.S.C. § 3161 . . . . .	53
18 U.S.C. § 3292 . . . . .	53

	PAGE
Fed. R. Crim. P. 17 . . . . .	22
Fed. R. Crim. P. 41 . . . . .	13, 22, 23, 25
S. Rep. No. 99-541 (1986). . . . .	10, 19, 29
H.R. Rep. No. 107-236 (2001) . . . . .	30
H.R. Rep. No. 99-647 (1986) . . . . .	10
<i>Wigmore on Evidence</i> (1961) . . . . .	57
J. Carr & P. Bellia, <i>The Law of Electronic Surveillance</i> (2004) . . . . .	29
Restatement (Third) of Foreign Relations Law § 442(1)(a) (1987) . . . . .	14, 45
Erin Bernstein and Theresa J. Lee, <i>Where The Consumer Is The Commodity: The Difficulty With The Current Definition Of Commercial Speech</i> , 2013 Mich. St. L. Rev. 39 (2013) . . . . .	43
Orin S. Kerr, <i>A User’s Guide to the Stored Communi- cations Act, and a Legislator’s Guide to Amending It</i> , 72 Geo. Wash. L. Rev. 1208 (2004) . . . . .	10, 13
Paul M. Schwartz, <i>Information Privacy in the Cloud</i> , 161 U. Pa. L. Rev. 1623 (May 2013) . . . . .	51
Cybercrime Convention Committee, <i>Transborder access and jurisdiction: What are the options?</i> (2002) . . . . .	46
<i>United States v. Paunescu</i> , 13 Cr. 41 (RPP), Indictment (S.D.N.Y. filed Jan. 17, 2013) . . . . .	50



**United States Court of Appeals**  
**FOR THE SECOND CIRCUIT**  
**Docket No. 14-2985**

---

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN  
E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY  
MICROSOFT CORPORATION

---

MICROSOFT CORPORATION,

*Appellant,*

—v.—

UNITED STATES OF AMERICA,

*Appellee.*

---

**BRIEF FOR THE UNITED STATES OF AMERICA**

---

**Preliminary Statement**

Microsoft appeals from orders entered on August 11, 2014, and September 8, 2014, in the United States District Court for the Southern District of New York, by the Honorable Loretta A. Preska, Chief United States District Judge, denying Microsoft's motion to vacate a warrant, issued pursuant to Title 18, United States Code, Section 2703, and holding Microsoft in contempt for non-compliance.

The warrant was issued on December 4, 2013, by the Honorable James C. Francis IV, United States Magistrate Judge, upon a finding that probable cause supported the compelled disclosure of emails and other data under Microsoft's control. Microsoft moved to vacate the warrant, arguing that it could not be ordered to produce the requested records because Microsoft stored them in a foreign country. Judge Francis denied Microsoft's motion on April 25, 2014, holding that Microsoft was not excused from producing records it controlled based on Microsoft's choice to store them abroad.

Microsoft challenged Judge Francis's decision in the District Court, but Chief Judge Preska rejected that challenge orally on July 31, 2014, and in a written order on August 11, 2014. Chief Judge Preska subsequently held Microsoft in contempt, pursuant to a stipulation between the parties, for failing to comply with the warrant.

Microsoft remains unwilling to produce the records named in the warrant.

## **Statement of Facts**

### **A. The Warrant Served on Microsoft**

Founded and headquartered in the United States, Microsoft is a provider of computer software, consumer electronics, and Internet-based services. Among its many offerings is a web-based email service available

to the public free of charge. (A. 35).<sup>1</sup> This service allows users anywhere in the world to establish an email account with Microsoft and use it to send and store messages. (A. 35-36).

On December 4, 2013, the Government presented Judge Francis with an affidavit establishing probable cause to believe that a Microsoft-based email account (the “Account”) was being used in furtherance of narcotics trafficking. (A. 48). After making an independent probable cause determination, Judge Francis issued a warrant (the “Warrant”), pursuant to the Stored Communications Act (the “SCA”), directing Microsoft “to disclose” any contents of the Account that were within “the possession, custody, or control of” Microsoft.<sup>2</sup> (A. 46).

Upon being served with the Warrant in the United States, Microsoft refused to disclose the records. It argued that the court could not compel Microsoft to disclose the contents of the Account because Microsoft stored them in its datacenter in Dublin, Ireland. (A. 36-37, 40). During the prior three years that the

---

<sup>1</sup> “A.” refers to the appendix filed with Microsoft’s brief on appeal; “Br.” refers to Microsoft’s brief; “Docket Entry” refers to an entry in the District Court’s docket; “[Name] Br.” refers to the brief filed by the named amicus curiae; and “Add.” refers to the addendum to this brief.

<sup>2</sup> The Warrant also directed Microsoft to provide other customer data that was stored in the United States and is not the subject of this appeal.

Dublin datacenter was in operation (A. 36), Microsoft never raised this objection as a basis to avoid compliance with the SCA.

Email accounts are assigned to the Dublin datacenter, according to Microsoft, based on the user's own uncorroborated identification of his or her country of residence at the time the account is created. (A. 36). The stated aim of this policy is to reduce the "geographic distance between a user and [the] datacenter" that services the account. (A. 36). Microsoft makes no effort, however, to verify the user's country of residence at the time of registration or at any time thereafter.<sup>3</sup>

Microsoft's decision to store email records in datacenters outside the United States does not deprive it of control over the records. Regardless of the storage location, the records remain readily available to U.S.-based Microsoft employees through a computer program that can "collect" the records from the datacenters where they are stored and import them into the United States. (A. 40). Using that program, Microsoft's U.S.-based compliance team is able to obtain records stored at any Microsoft datacenter anywhere in the world when responding to legal process. (A. 39-40). Moreover, Microsoft retains full control and discretion over the assignment of email accounts to

---

<sup>3</sup> Under this system, a U.S. citizen living in New York City could have his account hosted at the Dublin datacenter so long as he claimed to be a resident of Ireland.

datacenters within and outside the United States. (A. 37). A user appears to have no right under Microsoft's terms of service to demand that his data be stored at any particular datacenter or to object to its transfer from one datacenter to another.

### **B. The Proceedings Before the Magistrate Judge**

On December 18, 2013, Microsoft filed a motion with Judge Francis to vacate the Warrant. (A. 20-34). In support of its application, Microsoft maintained that the Warrant authorized an impermissible extra-territorial search of its datacenter in Dublin. (A. 28-32). The Government opposed the motion, arguing that the Warrant did not authorize a government official to enter the Dublin facility but instead compelled Microsoft, a U.S.-based entity, to produce records within its custody and control. (Docket Entry 9).

Following oral argument, Judge Francis denied Microsoft's motion. In a written opinion, Judge Francis held that the Warrant "lawfully obligated" Microsoft "to produce information . . . regardless of the location of that information." *In re Warrant to Search a Certain E-Mail Account*, 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014). That conclusion followed naturally from the statutory text of the SCA, which requires "a provider of electronic communication service[s] to disclose e-mail content" when the government has obtained a warrant authorizing that disclosure. *Id.* at 471. Judge Francis recognized that this power to order the disclosure of records was "not [an aspect of] a conventional warrant" but rather was a form of

compelled disclosure, created by statute and similar to a subpoena, requiring the recipient to deliver records, physical objects, and other materials to the government. *Id.*

Judge Francis then looked to this Court's precedents defining the scope of compelled disclosure and concluded that an entity can be ordered to disclose any "information in [its] possession, custody, or control regardless of the location of that information." *Id.* (citing *In re Marc Rich & Co.*, 707 F.2d 663, 667 (2d Cir. 1983)). Rejecting Microsoft's argument, Judge Francis held that the Warrant was not an extraterritorial assertion of U.S. law because "an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored." *Id.* at 475. All the Warrant requires is the production of records by an entity subject to U.S. jurisdiction, and that exercise of government power—even when reaching records stored abroad—is entirely consistent with longstanding precedent. *Id.* at 476 (citing *Blackmer v. United States*, 284 U.S. 421, 437 (1932)).

Having found no violation of the presumption against extraterritoriality, Judge Francis denied Microsoft's motion. *Id.* at 477.

### **C. The Proceedings Before the Chief District Judge**

Microsoft challenged Judge Francis's ruling by filing a series of objections with the District Court. (Docket Entry 15). In its submissions, Microsoft reiterated its position that the Warrant was an impermissible exercise of extraterritorial authority; it also pressed new arguments, including that the Warrant violated the Fourth Amendment's particularity requirement and that the records at issue were "owned" by the email user and not Microsoft itself.<sup>4</sup> (Docket Entries 15, 70).

On July 31, 2014, the parties appeared for oral argument. Microsoft relied heavily on the use of the word "warrant" in the statute as a basis to take "all of the territorial limitations" associated with conventional warrants and impose them on the type of warrant authorized by the SCA. (A. 331). The Government contested Microsoft's crabbed reading because it failed to account for the differences between a warrant authorized by the SCA, which is a form of compelled disclosure, and a conventional search warrant, which is not. (A. 284).

Following argument, Chief Judge Preska adopted Judge Francis's decision and held that "Congress intended in this statute for [electronic communications service providers] to produce information under their control, albeit stored abroad, to law enforcement in

---

<sup>4</sup> Microsoft appears to have abandoned its particularity argument on appeal.

the United States.” (A. 331-32). Chief Judge Preska also found that Microsoft had forfeited the argument that email content belongs to the users of its free email product, rather than to Microsoft, because it had not raised that argument before Judge Francis. (A. 332).

Pursuant to the parties’ stipulation and to “permit prompt appellate review,” Chief Judge Preska entered a contempt order against Microsoft for its continued refusal to comply with the Warrant.<sup>5</sup> (A. 342).

## **ARGUMENT**

### **The SCA Authorizes the Use of Warrants to Compel the Production of Records Regardless of Where They Are Stored**

The District Court properly directed Microsoft to comply with a valid court order to produce records within its custody and control. Challenging that decision, Microsoft contends that it need not do so because it stores the records abroad. This Court reject-

---

<sup>5</sup> The entry of a contempt order was necessary to ensure appellate jurisdiction. (A. 339). *See United States v. Punn*, 737 F.3d 1, 5 (2d Cir. 2013) (“To obtain appellate review, the subpoenaed person ordinarily must defy the district court’s enforcement order, be held in contempt, and then appeal the contempt order, which is regarded as final under § 1291.” (internal quotation marks omitted)).



ed that proposition 50 years ago, holding unequivocally that a corporation cannot resist compliance with a subpoena merely on the ground that the responsive records are stored abroad. In this litigation, Microsoft seeks to reopen the debate, relying on the fact that the court order at issue is statutorily labelled a “warrant,” rather than “subpoena,” “order,” or “summons.”

Microsoft’s argument is flatly contradicted by the explicit text of the statute, which requires service providers to disclose records when a warrant is obtained. Under the SCA, service providers are required to disclose records upon receipt of a subpoena, order, or warrant. Both the express language and statutory structure of the SCA make clear that a “warrant” issued under the statute functions as a form of compelled disclosure—that is, a court order requiring the recipient to disclose certain records. Under long settled precedent, the power of compelled disclosure reaches records stored abroad so long as there is personal jurisdiction over the custodian and the custodian has control over the records. Microsoft seeks to sidestep this precedent by claiming that the contents of the Account are not its own records and that complying with the Warrant will entail a conflict of laws. Neither the law nor the evidence supports Microsoft’s position.

In fighting nearly 50 years of settled law, Microsoft misconstrues the power exercised by the SCA, draws inapt analogies to forced entries of physical spaces, and raises the specter of international discord. Microsoft’s arguments crumble upon scrutiny, which is why they were swiftly rejected by both Chief

Judge Preska and Judge Francis. To adopt Microsoft's construction of the SCA would ignore the express text of the statute, abrogate well settled precedent in full accord with international norms, and disrupt the comprehensive disclosure scheme established by the SCA. Microsoft's preferred rule would do nothing to protect the civil liberties of email users, which are vindicated here by the time-tested requirement that a neutral magistrate find probable cause. What Microsoft's novel rule would do is deprive law enforcement of the ability to investigate and prosecute criminals using evidence obtained through a mechanism created by Congress and overseen by the courts.

## **A. Applicable Law**

### **1. The Stored Communications Act**

Congress enacted the SCA in 1986, as part of the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986). The statute was intended to extend privacy protections to emerging forms of telecommunications technology by setting conditions under which the government could compel service providers to disclose information under their control. *See* S. Rep. No. 99-541, at 1, 38-39 (1986); H.R. Rep. No. 99-647, at 68-69 (1986); *see generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-13 (2004).

The government's ability to compel the disclosure of records under the SCA is contained in the section

entitled “Required disclosure of customer communications or records.” 18 U.S.C. § 2703. It empowers the government to “require the disclosure” of records by electronic communications service providers, such as Microsoft. 18 U.S.C. § 2703(a)-(c). Under the statute’s comprehensive framework, certain compelled disclosures require a more demanding showing by law enforcement than others. The nature of that showing is determined by which instrument—subpoena, order, or warrant—is required to compel disclosure of the records in question.

At the low end of the spectrum is the subpoena, which the government can use to “require the disclosure” by a service provider of the following categories of information:

1. basic subscriber and transactional information concerning a user, 18 U.S.C. § 2703(c)(2);
2. contents of communications in electronic storage with a provider for more than 180 days, 18 U.S.C. § 2703(a) and (b)(1)(B)(i); and
3. other contents of communications stored by a remote computing service, 18 U.S.C. § 2703(b)(1)(B)(i).

These materials may be obtained through any “administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena.” 18 U.S.C. §§ 2703(b)(1)(B)(i) & (c)(2). The SCA does not require any prior judicial review, based

on either probable cause or reasonable suspicion, before the issuance of such subpoenas.

At the intermediate level is a court order pursuant to Title 18, United States Code, Section 2703(d) (a “2703(d) order”), which compels a service provider to disclose the following:

1. all records subject to production under a subpoena; and
2. any other “record or other information” concerning a user other than “the contents of communications,” such as historical logs of the email addresses in contact with the user, 18 U.S.C. § 2703(c)(1).

A 2703(d) order may be issued where the government provides a court with “specific and articulable facts showing that there are reasonable grounds to believe” that the records sought “are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

Finally, at the high end of the spectrum is a warrant (an “SCA warrant”) that authorizes government officials to “require the disclosure” by a service provider of the following records:

1. all records subject to production under a 2703(d) order (and therefore also a subpoena); and
2. contents of communications in electronic storage with a provider for *fewer than* 181 days, 18 U.S.C. § 2703(a).

Thus, with an SCA warrant, the government can obtain all email data in an account. An SCA warrant may be “issued using the procedures described in the Federal Rules of Criminal Procedure” which requires a judicial finding of probable cause based on a sworn affidavit. 18 U.S.C. 2703(a) & (b); *see* Fed. R. Crim. P. 41(d)(1) (requiring probable cause for warrants).

Under this framework, the information that is required to be disclosed depends on the instrument employed. Every category of information that the provider must disclose pursuant to a subpoena must also be disclosed pursuant to a 2703(d) order (plus additional categories); and every category of information that the provider must disclose pursuant to a 2703(d) order must, in turn, be disclosed pursuant to a warrant (plus additional categories). *See* 18 U.S.C. § 2703(b)(1)(A) and (c)(1)(A) (including a warrant among the instruments that can require the disclosure of records also available pursuant to a court order or subpoena). “The rules for compelled disclosure operate like an upside-down pyramid. . . . The higher up the pyramid you go, the more information the government can obtain.” Kerr, *A User’s Guide*, at 1222. In this fashion, records that Congress deemed entitled to greater privacy protection are more difficult to obtain than those afforded less protection. Notably, the language in the statute “requir[ing] . . . disclosure” by the provider remains the same regardless of the instrument employed.

## 2. The Compelled Production of Records Stored Abroad

Nearly fifty years ago, this Court observed, “It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has *in personam* jurisdiction of the person in possession or control of the material.” *United States v. First Nat. City Bank*, 396 F.2d 897, 900-01 (2d Cir. 1968). The passage of time has not weakened that holding. *See Linde v. Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (recognizing court’s power to order production of records stored abroad); Restatement (Third) of Foreign Relations Law § 442(1)(a) (1987) (“A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.”).

This authority is rooted in the longstanding principle that courts are empowered to exert authority on people and entities over whom they have jurisdiction, even if that authority has consequences overseas. *See, e.g., Blackmer v. United States*, 284 U.S. at 438 (“The jurisdiction of the United States over its absent citizen, so far as the binding effect of its legislation is concerned, is a jurisdiction *in personam*, as he is personally bound to take notice of the laws that are applicable to him and to obey them.”); *see also In re Marc Rich & Co.*, 707 F.2d 663, 667 (2d Cir. 1983) (recognizing that if court has “personal jurisdiction of

the summoned witness, the witness may not resist the summons on the sole ground that he is a non-resident alien” or “on the ground that the documents are located abroad” ); *cf. Hale v. Henkel*, 201 U.S. 43, 75 (1906) (“It would be a strange anomaly to hold that a state, having chartered a corporation to make use of certain franchises, could not, in the exercise of its sovereignty, inquire how these franchises had been employed, and whether they had been abused, and demand the production of the corporate books and papers for that purpose.”).

To determine whether a person or an entity can be ordered to disclose records, this Court has adopted a simple approach: “The test for the production of documents is control, not location.” *In re Marc Rich & Co.*, 707 F.2d at 667. Where a person or entity within the jurisdiction of a court has control over materials, government officials may order those materials to be produced. The type of control necessary to trigger this obligation “is not an esoteric concept.” *First Nat. City Bank v. I.R.S.*, 271 F.2d 616, 618 (2d Cir. 1959). For example, a corporation that has the “power to cause . . . records to be sent from a branch [office] to the home office for any corporate purpose[] surely has sufficient control to cause them to be sent on when desired for a governmental purpose properly implemented by a subpoena.” *Id.*

While a failure to disclose cannot be excused by the mere fact that records are stored abroad, courts are empowered to consider competing national interests when ordering the disclosure of materials located in foreign countries. This Court has long recognized

that it is not uncommon for “nations [to] hav[e] diametrically opposed positions with respect to the disclosure of a wide range of information” and that a “party or witness [might be] subject to the jurisdiction of two sovereigns and confronted with conflicting commands.” *United States v. First Nat. City Bank*, 396 F.2d at 901. When such genuine conflicts of law arise, courts are empowered to “weigh[] the conflicting legal obligations of U.S. discovery orders and foreign laws” on a case-by-case basis. *Linde v. Arab Bank, PLC*, 706 F.3d at 108. Courts conducting this analysis are to avoid “[m]echanical or overbroad rules of thumb [which] are of little value” and should instead apply “a careful balancing of the interests involved and a precise understanding of the facts and circumstances of the particular case.” *First Nat. City Bank*, 396 F.2d at 901.

Applying this teaching, courts have expressed “great reluctance” to excuse the compelled disclosure of records simply because of competing directives from foreign sovereigns. *Id.* at 903; *see Linde*, 706 F.3d at 109 (“[T]he operation of foreign law ‘does not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that law.’” (quoting *Societe Nationale Industrielle Aero-spatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n.29 (1987))). Particularly in the criminal context, courts have generally found that, even where foreign law prohibits the production of the relevant records, the powerful interest of the government in enforcing criminal law outweighs the foreign prohibition. *See, e.g., In re Grand Jury Proceedings (Bank of Nova Sco-*



*tia*), 740 F.2d 817, 826-29 (11th Cir. 1984) (production ordered despite Cayman Islands secrecy laws); *In re Marc Rich & Co.*, 707 F.2d at 665 (production ordered despite claim that it would violate Swiss law); *United States v. Vetco, Inc.*, 691 F.2d 1281, 1287-91 (9th Cir. 1981) (production ordered despite possible criminal penalties under Swiss law); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 547, 564 (S.D.N.Y. 2002) (Chin, J.) (production ordered even though prohibited by foreign laws and observing: “Courts consistently hold that the United States interest in law enforcement outweighs the interests of the foreign states in bank secrecy and the hardships imposed on the entity subject to compliance.”); *United States v. Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080, 1086-87 (S.D.N.Y. 1984) (production ordered pursuant to IRS summons despite Hong Kong bank secrecy orders).

## **B. Discussion**

### **1. The SCA Requires the Disclosure of Records by Warrant**

The SCA regulates compelled disclosure on a sliding scale, with the least sensitive information (basic subscriber information) available by mere subpoena and the most sensitive information (recent emails) available only upon the issuance of a warrant. But whether law enforcement agents obtain a subpoena, court order, or warrant, the mechanism for obtaining the records is the same: the service provider is required to disclose them.

The unambiguous text of the SCA authorizes the use of warrants to compel the production of records in a manner functionally similar to subpoenas, orders, summonses, and other instruments compelling the production of records. Under Section 2703(a), government officials may use a warrant to “require the disclosure” of communications “by a provider.” 18 U.S.C. § 2703(a); *see also In re Warrant to Search a Certain E-Mail Account*, 15 F. Supp. 3d at 468 (“The obligation of . . . Microsoft to disclose to the Government customer information or records is governed by the [SCA].” (emphasis added)). The SCA uses precisely the same language in describing how electronic communications may be obtained by way of subpoena or order. It provides that the government may “require the disclosure” of electronic communications *either* pursuant to a warrant *or*, for emails older than 180 days, pursuant to a subpoena or 2703(d) order. 18 U.S.C. § 2703(a) (“may require the disclosure by a provider”), (b)(1) (“may require a provider . . . to disclose”), (c)(1)(may require a provider . . . to disclose”), (c)(2) (A provider . . . shall disclose”).

As this Court has recognized in another context, “it would be needlessly untidy and confusing, absent good reason, to have one term mean two different things in a single statutory scheme.” *Drescher v. Shatkin*, 280 F.3d 201, 205-06 (2d Cir. 2002). Microsoft has identified no “good reason,” and the Government is aware of none, to believe that the “require[ment] of disclosure” has one meaning when applied to subpoenas and orders but an altogether different one when applied to warrants. The decision of Congress to use the same language for these three

instruments must be respected. Through this language, subpoenas, orders, and warrants are equally empowered to obtain records in the same way: through a disclosure requirement directed at a service provider.

The SCA's treatment of warrants as instruments of compelled disclosure has precedent. According to the original Senate Report, the disclosure provisions of the SCA were "modeled after the Right to Financial Privacy Act." S. Rep. No. 99-541, at 3. The Right to Financial Privacy Act also envisions that warrants—along with subpoenas and summonses—will trigger a disclosure requirement. That statute explicitly authorizes "financial records [to be] disclosed [by financial institutions] in response to a search warrant." 12 U.S.C. § 3402(3); *see also* 12 U.S.C. § 3406 ("A Government authority may obtain financial records . . . if it obtains a search warrant . . ."); *Duncan v. Belcher*, 813 F.2d 1335, 1339 (4th Cir. 1987) ("The government can obtain protected financial records if it obtains a subpoena, a search warrant, a court order, or the customer's written consent."). The SCA did not even chart new territory when it included warrants among the tools capable of requiring service providers to disclose records.

Microsoft, however, simply ignores that SCA warrants were designed to function as a form of compelled disclosure. As described by Microsoft, the Warrant is almost unrecognizable in its purported power to authorize federal agents to invade Microsoft's domestic and foreign facilities to gather evidence. (Br. 28 (The Warrant "authorizes a federal agent to

descend on Microsoft, demand entry, forcibly remove a technician at a terminal, and remotely access any Microsoft computer—in Dublin or anywhere else in the world”). At no point in the history of this litigation has the Government asserted the authority to use force to enter the Dublin datacenter. Microsoft’s vivid description of forced entry bears little resemblance to the power actually being exercised here: the power to “require” Microsoft to “disclose” records.

That power of compelled disclosure, contrary to Microsoft’s argument, is not altered by the fact that the Warrant was prepared using the generic template for search warrants, the so-called AO-93 form. (Br. 28-29). The Warrant could just as easily be prepared using a template for email warrants that contains none of the references to a physical entry that provide the basis for Microsoft’s argument. (Add. 1-5). Microsoft has never contended that it would comply with the Warrant if only it had been drafted from a different template. And if Microsoft was willing to do so, the Government would promptly reissue the Warrant and bring this litigation to an end. Microsoft’s refusal to comply with *any* warrant in *any* form that requires it to disclose records stored in the Dublin datacenter demonstrates that its arguments about the form of warrant are well beside the point.

To accept Microsoft’s reading of the statute is to embrace the notion that it does not matter what instruments actually do; all that matters is what they are named. That is why Microsoft must argue that a “warrant is directed toward a particular place to be searched or thing to be seized, rather than a person

who might possess or control the sought-after evidence.” (Br. 38). That description might very well apply to a traditional search warrant, authorizing law enforcement agents to forcibly enter and search physical places. But it does not describe the “warrant” issued here, pursuant to statutory authority that explicitly “require[s] the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication.” 18 U.S.C. § 2703(a).

At issue here is the nature of the power being exercised, not the way it is labeled. *See Bay Ridge, Inc. v. Fed’l Mine Safety & Health Review Comm’n*, 715 F.3d 631, 646 (7th Cir. 2013) (“For purposes of our Fourth Amendment analysis, we look to the substance of [the government’s] power rather than how the Act nominally refers to those powers.”). And the power being exercised under the SCA—whether the government is acting through a “warrant,” “order,” or “subpoena”—is functionally the same: it is the power to require the disclosure of records. That is why the District Court was right to dismiss Microsoft’s overreliance on the term “warrant” as excessively “simple, perhaps deceptively so.”<sup>6</sup> *In re Warrant to Search a Certain E-Mail Account*, 15 F. Supp. 3d at 470.

Other provisions of the SCA confirm that Congress intended to distinguish SCA warrants from

---

<sup>6</sup> Judge Francis’s memorandum order was adopted by Chief Judge Preska and is therefore referred to as the decision of the District Court.

more typical search warrants for physical locations issued under Rule 41 of the Federal Rules of Criminal Procedure. First, unlike Rule 41, which typically requires that a search warrant for a physical location be obtained in the district where the property is located, Fed. R. Crim. P. 41(b), the SCA has a separate, express jurisdictional provision that empowers any “court of competent jurisdiction” to issue an SCA warrant. 18 U.S.C. § 2703(b)(1)(A). This grant of jurisdiction is broader than the one in Rule 41, as it authorizes courts with “jurisdiction over the offense being investigated,” as well as those with jurisdiction over the physical location of the records and service providers, to issue SCA warrants. 18 U.S.C. § 2711(3). Under this authority, an SCA warrant can be obtained from any court that “has jurisdiction over the offense,” 18 U.S.C. § 2711(3), just as a federal criminal subpoena may be issued out of the investigating district and served anywhere the recipient is subject to service, *see* Fed. R. Crim. P. 17(e).<sup>7</sup>

Second, whereas a law enforcement officer must be present during execution of a physical search warrant and prepare an inventory of the seized property, the SCA specifically provides that a law enforcement

---

<sup>7</sup> Microsoft’s response that this provision does not allow for service “outside the United States” (Br. 26) misses the point. The Warrant does not seek to exert authority over an entity located abroad but is directed at Microsoft, a U.S. corporation subject to the personal jurisdiction of the U.S. District Court for the Southern District of New York.

officer need not be present at all for service or execution of an SCA warrant. *Compare* Fed. R. Crim. P. 41(f)(1)(B) *and* 18 U.S.C. § 3105 *with* 18 U.S.C. § 2703(g) (“the presence of an officer shall not be required for service or execution of [an SCA] warrant”). In practice, SCA warrants are most often served in the same manner as subpoenas—by faxing or otherwise transmitting them to the provider, which then must gather the material required to be disclosed.

Microsoft attempts to discount this provision, noting that it was enacted in 2002 after a district judge had attempted to impose an officer-presence requirement on SCA warrants the previous year. (Br. 40). *See United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002). In Microsoft’s view, the need to amend the statute proves that SCA warrants do not “oblige[] providers to produce their customer’s documents” in the manner of a subpoena because the presence of an officer is not required for subpoena compliance. (Br. 41). That interpretation of this sequence of events is, at a minimum, strained. It is far more plausible that the district judge’s erroneous construction of the SCA in *Bach* was so contrary to the intent of Congress that the statute was amended to bar any further impairment of the SCA’s efficacy.

After examining the substance of the Warrant, the District Court held that it was “not a conventional warrant” but instead “a hybrid: part search warrant and part subpoena.” *In re Warrant to Search a Certain E-Mail Account*, 15 F. Supp. 3d at 471. As the District Court correctly observed, an SCA warrant “is obtained like a search warrant when an application is

made to a neutral magistrate who issues the order only upon a showing of probable cause” but then “is executed like a subpoena in that it is served on the [provider] in possession of the information and does not involve government agents entering the premises of the [provider] to search its servers and seize the e-mail account in question.” *Id.* While Microsoft might dispute the District Court’s use of the term “hybrid” (Br. 39), it offers no explanation of how statutory text “requir[ing]” an entity “to disclose records” is the equivalent of forced entry into private spaces for the gathering of evidence.<sup>8</sup> That failure demonstrates how far afield Microsoft’s position is from the text of the SCA.

This does not mean that Congress’s choice to use the term “warrant” in the SCA is devoid of meaning. To the contrary, the District Court’s construction of the statute gives full meaning to Congress’s use of the term. The distinction Congress drew in the statute between warrants, orders, and subpoenas does not concern how these different instruments are executed or their geographic scope. Rather, the distinction con-

---

<sup>8</sup> It is no answer for Microsoft to point to 2703(d) orders as proof that the SCA’s drafters knew how to designate “novel” or “hybrid” instruments by using a “specific name” to identify them as such. (Br. 39). The term used in the SCA is entirely generic—“order” or “court order”—and not “(d) order” as Microsoft represents in its brief. (Br. 39-40). The substance of the order, as with the warrant, is defined in the text of the SCA.



cerns the requirements that must be met before they are issued. For records that Congress deemed most sensitive—emails less than six months’ old—the SCA requires the government to obtain a warrant “*issued* using the procedures described in the Federal Rules of Criminal Procedure.” 18 U.S.C. § 2703(a) (emphasis added). Unlike a subpoena or 2703(d) order, a warrant may issue only upon a finding of probable cause by a magistrate judge, based on a sworn affidavit of a law enforcement agent. *See* Fed. R. Crim. P. 41(d)(1). Congress thus sought to incorporate the same form of prior judicial review required for a physical search warrant, based on the heightened privacy interests it believed were implicated by emails in electronic storage for less than six months.

The purpose of the SCA’s warrant requirement was to extend the safeguards of the probable cause standard and prior approval by a neutral judge to recent emails, which Congress deemed worthy of special protections. But Congress did not mean to transplant every other feature of physical search warrants—in particular, their mode of execution—into the novel context of electronic communications stored by a provider. *See United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) (“Section 2703(a) refers only to the specific provisions of the Rules of Criminal Procedure, namely, Rule 41, that detail the *procedures* for obtaining and issuing warrants.”). And notwithstanding Microsoft’s argument (Br. 41), nothing in the Eighth Circuit’s observation that “Congress intended [SCA warrants] to be treated as warrants” is to the contrary. *United States v. Bach*, 310 F.3d at 1067 n.1. SCA warrants are treated like warrants in the way

they are applied for and issued by a neutral magistrate upon a showing of probable cause. But it is a fact—stated plainly in the text of the statute—that SCA warrants have the power to require the disclosure of records. To refuse to recognize that fact, as Microsoft does in this litigation, is to ignore the unambiguous text of the SCA.

**2. Nothing in the SCA’s Text, Structure, Purpose, or Legislative History Indicates that Compelled Production of Records Is Limited to Those Stored Domestically**

By authorizing the compelled production of records, the SCA empowers government officials to obtain records that U.S. service providers store abroad. Under settled precedent, so long as the entity with control over the records is subject to the jurisdiction of the court ordering their disclosure, the “test for the production of documents is control, not location.”<sup>9</sup> *In re Marc Rich & Co.*, 707 F.2d at 667. Microsoft ques-

---

<sup>9</sup> The name of the instrument used to obtain the records is not a factor in this analysis, as records have been obtained using various instruments, including those labelled subpoenas and summonses. *See, e.g., In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d at 826-29 (11th Cir. 1984) (subpoena); *United States v. Chase Manhattan Bank, N.A.*, 584 F. Supp. at 1086-87 (summons). The Government has found no authority for the proposition that the name of the instrument is relevant when determining whether records stored abroad must be produced.

tions whether SCA warrants have the same “geographic scope” as subpoenas issued under the same statutory scheme. (Br. 39). But nothing in the SCA’s text, structure, purpose or legislative history provides any basis to conclude that subpoenas and orders issued under the statute may compel the production of records stored abroad, while warrants cannot.

As described in the previous section, subpoenas, orders, and warrants issued under the SCA can all be used to compel disclosures from service providers. Once the appropriate instrument is obtained, its power is the same: each one requires disclosure by a service provider. *See* 18 U.S.C. § 2703(a) (“may require the disclosure by a provider”), (b)(1) (“may require a provider . . . to disclose”), (c)(1)(may require a provider . . . to disclose”), (c)(2) (A provider . . . shall disclose”). Nothing in the relevant statutory text suggests, much less states explicitly, that the power of one of these instruments is broader or narrower in geographic scope than another.

Microsoft believes that this silence weighs in its favor because Congress should have stated explicitly that it intended to invest SCA warrants with the same geographic reach as that of subpoenas. (Br. 39). Microsoft has it exactly backward. At the time the SCA was enacted in 1986, it was a settled point of law that compulsory process could reach records stored overseas—a point of law that we presume Congress understood when it legislated. *See Cannon v. Univ. of Chicago*, 441 U.S. 677, 696-97 (1979). Thus, when the drafters of the SCA chose to speak in terms of compelled disclosure, they legislated against

the background principle that compelled disclosure extends to records stored overseas. In the absence of any explicit geographic restrictions in the statutory text, there is no basis to conclude that the geographic scope of warrants authorized by the SCA is narrower than that of subpoenas authorized by the same statutory provisions using the same statutory language.

A geographic restriction would also run counter to the structure of the SCA. Under Microsoft's reading of the SCA, a subpoena could be used to compel disclosure of records (such as email stored abroad for more than 180 days) that could not be compelled with a warrant. Because the emails sought in this investigation are now more than 180 days old, the plain language of the SCA would authorize the government to use a subpoena to compel disclosure of everything it sought pursuant to the Warrant.<sup>10</sup> If Microsoft is right, Congress created a framework under which

---

<sup>10</sup> Microsoft argues that the SCA is unconstitutional to the extent it permits the compelled disclosure of email without a warrant. (Br. 47-48 (citing *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)). The *Warshak* decision, which was issued nearly a quarter century after the SCA was enacted, does not shed any light at all on what Congress intended when it passed the SCA. For the purpose of understanding the framework for compelled disclosure that Congress created when it enacted the SCA, *Warshak* is irrelevant, except to the extent it recognizes that Congress intended to authorize the use of subpoenas to require the disclosure of emails.

government agents would be able to obtain more email using a subpoena than could be obtained using a warrant. Not only does this reading of the statute run counter to common sense, it also conflicts with the SCA's structure, under which any information available through less rigorous legal process (a subpoena or order) is also available through more demanding process (a warrant). *See* J. Carr & P. Bellia, *The Law of Electronic Surveillance* § 4:80 (2004). It would also place certain records—emails stored abroad that are less than six months' old—beyond the reach of the statute entirely, even upon a finding of probable cause by a neutral magistrate. Nothing in the framework created by the SCA suggests that any category of information is exempt from its comprehensive disclosure regime, much less this particular category.

It is even harder to understand how this supposed carve-out would further the SCA's purpose. The SCA was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment. *See* S. Rep. No. 99-541, at 5. That purpose is not furthered by restricting the geographic scope of mandated disclosures for warrants, which require the most rigorous judicial showing, but not subpoenas, which require no judicial findings at all. There is nothing inherently more private or sensitive in recent emails stored abroad than in those stored within the United States. And the fact that the emails are stored abroad is not the relevant factor because it is only recent emails that would fall within the purported exemption: the statute requires disclosure of emails older than 180 days by subpoena and

2703(d) order, even if stored in a foreign location. The incompatibility of Microsoft's desired result with the purpose of the SCA demonstrates that the imposition of a warrant requirement has nothing to do with the physical location of the relevant records. It has everything to do with ensuring that sensitive records are disclosed only upon a more rigorous investigative showing: prior approval by a neutral magistrate upon a finding of probable cause.

Furthermore, nothing in the legislative history of the SCA indicates that Congress intended to impose geographic limits on warrants issued under the statute. Misreading the legislative history, Microsoft points to a 2001 amendment expanding jurisdiction to issue SCA warrants, which it argues "reinforced [the] territorial limitations" of those warrants. (Br. 25 (citing Pub. L. 107-56 § 220, 115 Stat. 272 (2001))). The amendment authorized courts with "jurisdiction over the offense being investigated" to issue SCA warrants, 18 U.S.C. § 2711(3)(A)(i), but it says nothing about the locations where a provider must subsequently collect records when responding to such a warrant. The effect of this amendment was to broaden—not narrow—the power of courts to issue SCA warrants by not tethering them to the district where the records happened to be stored. *See* H.R. Rep. No. 107-236, at 57 (2001) (explaining that the amendment eliminated the "requirement that the 'warrant' be obtained 'within the district' where the property is located," in order to "address the investigative delays caused by the cross-jurisdictional nature of the Internet"). The amendment shows that Congress sought to allow the government to obtain SCA warrants free

from concerns about where a provider decided to store responsive information.

### **3. Compliance with the Warrant Does Not Implicate the Presumption Against Extraterritoriality**

Recognizing the incompatibility of its position with precedent, Microsoft challenges the proposition that the test for compelled disclosure is control, not location—the same proposition this Court deemed “no longer open to doubt” fifty years ago. *First Nat. City Bank*, 396 F.2d at 900. Microsoft argues that this well settled precedent “teeters on unsteady ground” following the Supreme Court’s decision in *Morrison v. Nat’l Austl. Bank Ltd.*, 561 U.S. 247 (2010). (Br. 52). This argument is unfounded.

*Morrison* held that U.S. securities laws cannot provide a cause of action where the relevant securities are not “listed on a domestic exchange” and where “all aspects of the purchases [of securities] . . . occurred outside the United States.” *Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. at 273. Applying the presumption against extraterritoriality, *Morrison* makes clear that the substantive protections of U.S. securities laws apply only to domestic U.S. securities transactions. *See id.* at 266 (substantive prohibition of “deceptive conduct” applies only to domestic transactions). But Microsoft’s challenge to the Warrant has nothing to do with the substantive provisions of any U.S. law.

The relevant inquiry here concerns the extent of a U.S. court’s power to compel Microsoft, a U.S. compa-

ny, to disclose records in its possession, custody, and control. That power is based on the court's personal jurisdiction over Microsoft. And the scope of this judicial power is generally not cabined by presumptions about the intended geographic reach of legislation.<sup>11</sup> *See, e.g., United States v. First Nat'l City Bank*, 379 U.S. 378, 384 (1965) ("Once personal jurisdiction of a party is obtained, the District Court has authority to order it to 'freeze' property under its control, whether the property be within or without the United States."). Here, a neutral magistrate judge issued the Warrant to compel an entity within the court's jurisdiction to disclose its records to law enforcement officials in the United States. And Microsoft does not dispute that it is subject to the District Court's jurisdiction.

As for the substantive law in question, Microsoft has never challenged the Government's authority to investigate and prosecute the user of the Account for a violation of U.S. narcotics laws. This litigation therefore has nothing to do with the application of the substance of U.S. laws abroad. Rather, it has to do with the scope of compelled disclosure to gather evidence when investigating a violation indisputably

---

<sup>11</sup> The presumption against extraterritoriality pertains to the geographic reach of substantive provisions of U.S. law. *See Morrison*, 561 U.S. at 255. The purpose of this presumption is to "protect against unintended clashes between our laws and those of other nations." *United States v. Vilar*, 729 F.3d 62, 74 (2d Cir. 2013).



within the territorial reach of U.S. authorities. Neither *Morrison* nor the presumption against extraterritoriality has anything to say about a court's power to compel the production of evidence from abroad where there is no dispute that the substantive provisions of U.S. law apply.

Microsoft responds that the Warrant compels it to undertake a search for and seizure of evidence, in effect “conscript[ing]” it “to copy emails” from the Dublin datacenter as the government’s agent. (Br. 30). But the Warrant simply requires Microsoft to disclose to law enforcement agents (in the United States) records under its control—regardless of where those records are stored. The fact that Microsoft happens to store records responsive to the Warrant overseas does not render the SCA “extraterritorial” in any impermissible sense. Were the law otherwise, the internal revenue code would be equally invalid any time a corporation must transfer funds held abroad to the United States in order to pay its taxes. *See Envtl. Def. Fund. v. Massey*, 986 F.2d 528, 531-32 (D.C. Cir. 1993) (“Even where the significant effects of the regulated conduct are felt outside U.S. borders, the statute itself does not present a problem of extraterritoriality, so long as the conduct which Congress seeks to regulate occurs largely within the United States.”). The concern of the presumption against extraterritoriality is with the substance of laws reaching beyond U.S. borders, not the overseas consequences of U.S. laws applied domestically.

Moreover, Microsoft is wrong to characterize the Warrant as deputizing it to conduct a search and sei-

zure on behalf of the government. Quite to the contrary, just like a subpoena, the Warrant simply requires the disclosure of specific records under Microsoft's control. An order merely compelling the production of records does not confer any authority on the responding entity to conduct any sort of investigation for the government. *See, e.g., In re Search*, 13 F. Supp. 3d 157, 165 (D.D.C. 2014) (noting that SCA warrant did not require service provider to “search through e-mails and electronic records related to the target account and determine which e-mails are responsive”). That is why the Supreme Court has long recognized that the “Fourth Amendment was not intended to interfere with ‘the power of courts to compel, through a *subpoena duces tecum*, the production, upon a trial in court, of documentary evidence,’” *United States v. Bausch & Lomb Optical Co.*, 321 U.S. 707, 727 (1944) (quoting *Hale v. Henkel*, 201 U.S. at 73), and that ordering an entity to disclose records “present[s] no question of actual search and seizure” where there is no attempt to “enter [the entity’s] premises against [its] will, to search [it], or to seize or examine [its] books, records or papers without [its] assent.” *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 195 (1946). The act of gathering records by an entity with custody and control over those records does not amount to a government search or seizure at the time the records are gathered.<sup>12</sup>

---

<sup>12</sup> Cases, like this one, that involve the required disclosure of records already in an entity’s control are easily distinguished from cases like *Skinner v. Rail-*

This is not to say that there are no constitutional limits on the government's power to compel the disclosure of information. The Supreme Court has recognized that "subpoenas which suffer from too much indefiniteness or breadth" may be appropriately quashed. *Fisher v. United States*, 425 U.S. 391, 401 (1976). And, of course, an entity cannot be ordered to produce items that are not within its custody or control, or that are subject to privilege. But an entity's compliance with an order to disclose records within its control does not cause that entity to be the agent of a government seizure. Were it otherwise, every subpoena the government has ever issued would constitute a "search" and "seizure" under the Fourth Amendment at the time the responding party gathers records under its control without government participation or oversight. That is not and has never been the law.<sup>13</sup>

---

*way Labor Executives Ass'n*, 489 U.S. 602, 614 (1989), in which a private entity conducted blood and urine tests of a third party at the direction of the government.

<sup>13</sup> Despite Microsoft's urging (Br. 31-32), this Court's recent decision in *United States v. Ganius* does not suggest otherwise. 755 F.3d 125 (2d Cir. 2014). In *Ganius*, this Court held that there was a government seizure under the Fourth Amendment when government agents retained a copy of a hard drive after the agents' authority to possess the data had ended. *Id.* at 137. That case had nothing to do with the compelled disclosure of records by a third

Even if the presumption against extraterritoriality described in *Morrison* were relevant to this appeal, which it is not, Microsoft recognizes that this Court has already held that compulsory process reaches records stored abroad, and that decision remains the binding law of this Circuit. (Br. 53 n.6). As this Court has frequently stated, precedential decisions must be followed “until such time as they are overruled either by an *en banc* panel of [this] Court or by the Supreme Court.” *United States v. Wilkerson*, 361 F.3d 717, 732 (2d Cir. 2004). This doctrine provides yet another basis for rejecting Microsoft’s suggestion that *Morrison* has secretly undermined long settled precedent on the geographic scope of compelled disclosure. The argument can be safely set aside.

#### **4. The Warrant Can Compel Microsoft to Produce Emails in the Account Regardless of Who “Owns” Them**

Pressing an argument that Chief Judge Preska ruled forfeited, Microsoft submits that compelled production can reach only an entity’s own business records and not records it holds on behalf of others whose Fourth Amendment rights are at stake.<sup>14</sup>

---

party. The questions of when the seizure occurred and who was an agent accomplishing the seizure, which Microsoft presses here, were not at issue, much less decided in *Ganias*.

<sup>14</sup> This argument has not been preserved for appeal, as Chief Judge Preska concluded that Microsoft forfeited this objection to the Warrant by failing to

(Br. 41-42). If this argument is considered on the merits in this appeal, rather than deemed forfeited, it should still be rejected. Not only is the argument unsupported by any facts in the record, it is, more importantly, wrong on the law, for nothing prohibits the Government from using compulsory process to obtain Fourth Amendment-protected records under the control of a third party.

Assuming for the sake of argument that Microsoft serves as nothing more than a caretaker of the Account and that the Account is protected by the Fourth Amendment, precedent would still require Microsoft to produce the records. While Microsoft submits that an entity can be ordered to produce only its “own” business records stored abroad (Br. 43), neither the Supreme Court nor this Court has ever recognized such a restriction. In fact, precedent demonstrates otherwise—that the test for compelled production of records is, again, simply “control,” rather than an as yet undefined concept of corporate “ownership” of records. And the fact that the instrument used to compel disclosure is a warrant satisfies any Fourth Amendment interest of the account holder.

In *United States v. First National City Bank*, for example, this Court addressed the propriety of a subpoena seeking two categories of records: “material entrusted to a bank within the framework of [a] confi-

---

raise it before Judge Francis. (A. 332). That failure alone would provide a sufficient basis to reject Microsoft’s position.

dential relationship” and “records that were the bank’s own work product.” 396 F.2d at 900 n.8. In other words, the subpoena sought confidential customer records entrusted to the bank (as Microsoft claims the Warrant seeks from it here) and records generated by the bank in the course of its own business. The Court ordered disclosure of both. *Id.* at 905. Both categories of records were stored by the bank abroad, and both were required to be disclosed. *Id.* That precedent stands in stark contrast to Microsoft’s assertion that the subpoena power may be used to obtain only an entity’s “own” records.

Other precedent confirms there is no obstacle to using compelled disclosure to obtain someone’s private records from a third party. *In re Horowitz* called on this Court to decide whether a subpoena could compel an accountant to produce three locked filing cabinets entrusted to him by a client fleeing prosecution. 482 F.2d 72, 74 (2d Cir. 1973). Some of the records in the locked cabinets had been used by the accountant in performance of his duties, but “others were personal records, some taken from [the client’s] home, which were unrelated to [the accountant’s] role.” *Id.* at 83. The accountant, much like Microsoft, had the ability to access the contents of all three cabinets. *Id.* at 74. This Court, in a decision written by Judge Friendly, held that the cabinets had to be produced pursuant to the subpoena, albeit with a date-range restriction having nothing to do with the distinction Microsoft draws between a business’s own records and its client’s. *Id.* at 87.

Similarly, this Court and district courts in this Circuit have approved the use of a subpoena to obtain containers of records held by third-party custodians, to be followed by search of the records inside upon a showing of probable cause. In *United States v. First National City Bank* (separate from the similarly captioned case described above), a bank was ordered to turn over the contents of a safe deposit box pursuant to an administrative subpoena. 568 F.2d 853, 855 (2d Cir. 1977). This Court found nothing improper in the use of that instrument to obtain control over the box because, before the contents of the box were examined, “a detached magistrate [had] determine[d] [that] there [was] sufficient probable cause for the search.” *Id.* at 858.

Likewise in *United States v. Barr*, the government used a grand jury subpoena to compel an entity that “receive[d] mail and telephone messages” to disclose the content of mail and messages it held for one of its clients. 605 F. Supp. 114, 116 (S.D.N.Y. 1985). After receiving that disclosure, the government obtained a search warrant and then “opened the mail” obtained pursuant to the subpoena. *Id.* The District Judge found the use of a subpoena to obtain the unopened mail entirely proper. *Id.* at 118-19; *see also United States v. Giovanelli*, 747 F. Supp. 891, 895 (S.D.N.Y. 1989) (approving use of subpoena to “preserve” safe deposit boxes while warrants obtained).

As these precedents show, courts have repeatedly approved the compelled disclosure of records held on behalf of others, particularly where the subsequent review of those records is pursuant to prior judicial

approval under a probable cause standard. And that is precisely analogous to the procedure contemplated by an SCA warrant: compelled disclosure followed by a review of the records, all of which is authorized by a neutral magistrate upon a showing of probable cause. Such a procedure is appropriate regardless of who “owns” the records. Microsoft’s complaints that it holds the requested records “in trust” and has “limited control over the emails” is simply beside the point.

Microsoft resists this logic by pointing to this Court’s decision in *United States v. Guterma*, 272 F.2d 344, 346 (2d Cir. 1959), quashing a subpoena ordering the production of a locked safe by a custodian who did not have its combination. (Br. 46-47). That case only underscores that control—not “ownership”—is the determinative test. The “most significant” fact in that case was the subpoena recipient’s “lack of access to the safe.” *United States v. Guterma*, 272 F.2d at 346. Because of that lack of access, the defendant in the underlying criminal matter would have had to unlock the safe and, in effect, “deliver his own papers,” which this Court held would run afoul of the Fifth Amendment’s act of production privilege; therefore, the Court excused compliance with the subpoena. *Id.* That highly fact-specific holding has nothing to do with the facts here, as Microsoft “knows” the “combination” to the Account and has not invoked the act of production privilege (nor could



it).<sup>15</sup> Microsoft's inability to find any relevant authority supporting its crabbed understanding of the scope of compelled disclosure demonstrates that its understanding is mistaken.

Even if Microsoft's position had support in precedent, the factual record would remain an insurmountable barrier for Microsoft for at least two reasons. First, Microsoft's claim that it is nothing more than a "caretaker" for the email in the Account, which it claims to hold "in trust" for the user (Br. 41-42) finds no support in the evidentiary record. At no point in the proceedings before Chief Judge Preska or Judge Francis did Microsoft introduce into the record the terms of service that governed its email offering at the time the Account was opened and used. That omission may well have been intentional, as the terms of service currently applicable to Microsoft's free email service do not suggest a mere caretaker or trust relationship. Rather, they assert Microsoft's right to access or use the *contents* of its customers' emails:

---

<sup>15</sup> *Guterman* was also decided before the Supreme Court abolished the "mere evidence" rule that limited the government's authority to seize items that were not "fruits, instrumentalities, or contraband" of crimes. *Warden v. Hayden*, 387 U.S. 294, 310 (1967). Thus, it was decided before the government could use the combination of a subpoena and warrant to compel disclosure of and then search a closed container containing evidence.

- “When you transmit or upload Content [*i.e.*, the text of emails] to the Services, you’re giving Microsoft the worldwide right, without charge, to use Content as necessary: to provide the Services to you, to protect you, and to improve Microsoft products and services.”
- To ensure that users comply with Microsoft’s “Code of Conduct,” Microsoft uses “automated technologies” to review the content of emails, and separately, when “investigating” possible violations, “Microsoft or its agents will review Content in order to resolve the issue.”<sup>16</sup>

Microsoft Services Agreement (effective July 31, 2014), at <http://windows.microsoft.com/en-us/windows/microsoft-services-agreement>. These terms of service would appear incompatible with Microsoft’s assertion that it is nothing more than a “limited custodian” analogous to “banks and mail carriers.” (Br. 46).<sup>17</sup>

---

<sup>16</sup> Notably, Microsoft reserves the right to conduct this review of emails (presumably without probable cause or prior judicial approval) in order to investigate possible violations of its Code of Conduct, while simultaneously refusing to disclose emails to the government pursuant to a court-issued warrant directed at criminal violations of Title 21 of the United States Code.

<sup>17</sup> Other providers of free Internet-based services routinely capture, compile, and sell user information

Second, Microsoft assumes that the contents of the Account are protected by the Fourth Amendment. (Br. 44-47 (repeatedly citing *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)).<sup>18</sup> But such a finding would require a more thorough analysis of a better developed record.<sup>19</sup> In particular, the Supreme Court has held that “the Fourth Amendment has no application” to the search of property outside the United States belonging to a non-U.S. citizen “with

---

to marketers. *See, e.g.*, Erin Bernstein and Theresa J. Lee, *Where The Consumer Is The Commodity: The Difficulty With The Current Definition Of Commercial Speech*, 2013 Mich. St. L. Rev. 39, 40-41 (2013) (“These services are free to users. But, as many shrewd commentators have noted, when users don’t pay for a product, often the user is the product. That is, companies like Google and Facebook develop a large user base by offering free services and then ‘sell against’ that user base to advertisers, venture capitalists, and other financial backers.” (footnotes omitted)). Such providers would be even more hard-pressed to claim that they are simple “custodians.”

<sup>18</sup> *Warshak* is not relevant to the issues presented here, but if it were, it would neither bind the Government nor this Court. And, in any event, *Warshak* would be fully satisfied here because a warrant was obtained.

<sup>19</sup> Whether and to what extent the Fourth Amendment applies is a fact-dependent inquiry. *See Minnesota v. Carter*, 525 U.S. 83, 88 (1998).

no voluntary attachment to the United States.” *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990). Here, the parties do not dispute that the records at issue are stored abroad, and nothing in the record of this case establishes whether the user of the Account is a U.S. citizen or has any substantial ties to the United States. Microsoft has therefore failed to develop a factual record showing that these records are entitled to protection under the Fourth Amendment.

To affirm the District Court’s orders, this Court need not resolve these open factual issues. Even assuming that the contents of the Account are held in trust by Microsoft and are subject to Fourth Amendment protection, the law is clear that the Government may use compulsory process to obtain Fourth Amendment-protected records in the custody of a third party. And insofar as the user’s privacy interests are concerned, they have been appropriately protected by the fact that the government has obtained a warrant, based on a showing that there is probable cause to believe the user’s account contains evidence of a crime—which is all the Fourth Amendment could require.

##### **5. Compliance with the Warrant Does Not Implicate Any Genuine Conflict of Laws That Would Raise Comity Concerns**

This Court has long empowered district judges to take into account the competing claims of foreign sovereigns when evaluating challenges to compelled disclosures. *See, e.g., United States v. Davis*, 767 F.2d

1025, 1034 (2d Cir. 1985) (summarizing relevant factors). However, there is no genuine conflict of laws at issue in this case. Microsoft does not argue that complying with the Warrant would require it to violate the law of Ireland or of the European Union.<sup>20</sup> Microsoft argues vaguely that its compliance with the Warrant would be “offensive to foreign sovereignty” (Br. 51) but supports its argument only with statements of opinion by individual foreign politicians and “[f]oreign newspapers.” (Br. 13-14). Such statements do not give rise to any cognizable comity concern and are entirely insufficient to overcome the Government’s powerful interest in obtaining evidence of criminal activity.

As an initial matter, Microsoft claims that the compelled production of records stored abroad is an affront to international norms (Br. 1-3, 18, 34-35, 52), but that is demonstrably false. In fact, international norms have long recognized that a sovereign retains the authority to order an entity within its jurisdiction to repatriate records. (BSA Br. 17 & n.5 (describing U.K. legislation authorizing warrants “compel[ling] the disclosure of content” stored abroad); *see also* Restatement (Third) of Foreign Relations Law § 442(1)(a) (1987) (“A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to pro-

---

<sup>20</sup> Notably, Microsoft’s Dublin datacenter has been operational since September 2010 (A. 36), but Microsoft never refused compliance with an SCA warrant on that basis until now.

duce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.”). Most importantly, Ireland itself has recognized this norm. Its Supreme Court has upheld the compelled “disclosure by an Irish corporation of information in its possession, notwithstanding that the information is physically located in another jurisdiction.” (Ireland Br. 7). Microsoft is simply wrong to claim that the compelled disclosure of records violates international norms.<sup>21</sup>

Microsoft has equally failed to establish that compliance with the Warrant would violate Irish data privacy laws. (Br. 52). Throughout this litigation, Microsoft has been free to introduce evidence in support of such an argument, but its evidence has fallen far short of the mark. In the proceedings below, Microsoft submitted a letter, in which a European politician expressed “concern” that Microsoft’s compliance with the Warrant “*may* be in breach of interna-

---

<sup>21</sup> In fact, a recent study prepared by the Council of Europe documents the powers claimed by many European countries to seize electronic evidence directly, even when it is stored within the territory of other countries. See Cybercrime Convention Committee, *Transborder access and jurisdiction: What are the options?* (2002), at ¶¶ 167-70 (Belgium), ¶ 194 (Norway), ¶¶ 199-200, 202 (Portugal), ¶ 226 (Serbia), [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY\\_2012\\_3\\_transborder\\_rep\\_V31public\\_7Dec12.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf).

tional law.” (A. 151 (emphasis added)). However, nothing in that letter states that compliance with the Warrant would violate Irish or European law, let alone cause Microsoft to be subject to any penalties for doing so. Notably, in its amicus brief, Ireland does not state that either its sovereignty or any of its laws would be violated by Microsoft’s compliance with the Warrant.<sup>22</sup>

Microsoft also submitted declarations from an Irish attorney, but those submissions are more illuminating for what they do not say than for what they do. (A. 114-17, 262-63). The Irish attorney does not opine that Irish law would subject Microsoft to either criminal or civil penalties were it to comply with the Warrant. Instead, he notes that disclosures may be made under “certain particular exceptions” without saying whether any of those exceptions are applicable here. (A. 116). Indeed, at oral argument before Chief Judge Preska, the Government invited Microsoft to identify “any specific provision of Irish law that in any way forbids it from handing the data over.” (A. 317). Microsoft offered no response. With no conflict of law argued or identified, Microsoft’s concern for comity is more rhetorical than real. The District Court was correct to reject these “speculative” concerns as insufficient to excuse Microsoft from compliance with the Warrant. *First Nat. City Bank*, 396

---

<sup>22</sup> The record does not even indicate whether the user of the Account is connected in any fashion to Ireland separate from Microsoft’s unilateral decision to store his emails there.

F.2d at 905. This Court should reach the same conclusion.

**6. Policy Considerations Weigh Against Creating an Easily Abused Loophole in the SCA's Comprehensive Disclosure Requirements**

When construing the meaning of a statute, this Court will “look not only to the particular statutory language, but also to the design of the statute as a whole and to its object and policy.” *Johnson v. United States*, 123 F.3d 700, 702-03 (2d Cir. 1997). It is therefore entirely “appropriate” to examine the “practical consequences of the suggested interpretations” when attempting to determine which interpretation is nearest the one Congress intended. *Id.* at 703. Notwithstanding this precedent, Microsoft would prefer that this Court ignore the practical consequences of Microsoft’s reading of the SCA. (Br. 54-56). That is for good reason: adopting Microsoft’s view would undermine the SCA’s comprehensive disclosure scheme, severely impair the investigation and prosecution of criminals, and do nothing to advance the privacy interests of email users.

Microsoft and amici principally argue that the government should be required to rely on mutual legal assistance treaties (“MLATs”), rather than the compelled disclosure provisions of the SCA, when seeking records stored abroad. (Br. 57-58; Digital Rights Br. 20-25; Albrecht Br. 9-10). There are at least four flaws in this argument. First, there is nothing in international law that requires the government



to use an MLAT to obtain evidence located in a foreign country when other lawful means of obtaining the evidence are available. See *In re Grand Jury Subpoena*, 646 F.3d 159, 165 (4th Cir. 2011) (finding that MLAT was “not the exclusive means for the government to obtain documents from a party located in [a foreign] country”); *United States v. Rommy*, 506 F.3d 108, 129 (2d Cir. 2007) (finding that MLAT had “no application to evidence obtained outside the MLAT process”); cf. *United States v. Alvarez-Machain*, 504 U.S. 655, 664-67 (1992) (holding that a treaty does not prohibit actions “outside of its terms” where it “does not purport to specify the only way” in which the United States may accomplish a task); *Societe Nationale Industrielle Aerospatiale*, 482 U.S. at 542-43 (“A rule of first resort in all cases would therefore be inconsistent with the overriding interest in the just, speedy, and inexpensive determination of litigation in our courts.” (internal quotation marks omitted)). Microsoft’s view would upend these precedents and effectively *require* the Government to use an MLAT even though the SCA provides a far more efficient means of obtaining the relevant evidence.<sup>23</sup>

---

<sup>23</sup> Microsoft’s rule would also deprive treaty parties of the power to negotiate terms of their choosing. While some countries do in fact negotiate treaties that require that the treaty mechanism must be used when available, the MLATs at issue here contain neither exclusivity nor “first-use” provisions. In this case, Microsoft has asserted that the records at issue are stored in Ireland. Ireland and the United States

Second, most countries in the world do not have MLATs with the United States, and some MLATs are topic-restricted. A U.S. provider could easily choose to locate its user data in such a country either for legitimate business reasons or for the specific purpose of evading the reach of U.S. law enforcement.<sup>24</sup> Such data would remain largely outside the court's power and the prosecutor's reach even if the emails were sent by

---

have agreed to assist one another in gathering evidence, but have chosen not to require that the treaty be used if other means are available. Microsoft proposes that countries should not be free to negotiate a mutually satisfactory arrangement on this point by reading in a first-use provision every time. (Br. 59-60; Colangelo Br. 27-30). Microsoft's judgment about when the use of an MLAT should be required cannot be substituted for the judgment of the actual parties to such treaties.

<sup>24</sup> Indeed, some providers less scrupulous than Microsoft may do so with the specific intent to accommodate criminal users. *See, e.g., United States v. Paunescu*, No. 13 Cr. 41 (RPP), Indictment (S.D.N.Y. filed Jan. 17, 2013) (bringing charges under 18 U.S.C. § 1030(b) against operator of "bulletproof hosting service," who, "in exchange for fees, . . . provided cyber criminals with Internet Protocol . . . addresses and servers in a manner designed to enable them to preserve their anonymity and evade detection by law enforcement").

U.S. citizens within the United States and there was probable cause to believe that criminal activity was afoot.<sup>25</sup> There is no reason to believe that Congress intended to exclude such plainly relevant evidence from the comprehensive disclosure framework established by the SCA.

Third, even when MLATs are available, they may be entirely ineffective if the records do not reside in any single country for very long. For example, a provider might move a particular user's data between servers in multiple countries for any number of reasons, including network maintenance or load-balancing reasons, a practice that is becoming increasingly common with the growth of cloud computing. See Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. Pa. L. Rev. 1623, 1629 (May 2013) (“[C]loud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm.” (internal quotation marks omitted)). In this case, for example, a Microsoft engineer described how “[s]everal times each day, Microsoft's backend software runs an automatic scan to determine whether newly-created accounts should be migrated to the Dublin datacenter.” (A. 37). In light of this ease of

---

<sup>25</sup> In the absence of an MLAT, the government would be forced to rely on antiquated processes such as letters rogatory, the execution of which may depend on the discretion and willingness to assist of the recipient.

mobility, the government would find itself unable to anticipate where data might reside at the time an MLAT could be served, and therefore unable to use an MLAT to compel the production of records. SCA warrants do not suffer from that limitation. They require providers, who know and control the location of the records, to disclose them upon receipt of a subpoena, order, or warrant.

Fourth, resort to an MLAT will hardly ever result in as prompt a disclosure of records as is available with an SCA warrant. In contrast to an SCA warrant, which can be served upon a provider immediately upon issuance by a judge, an MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system.<sup>26</sup> *See, e.g., In re Grand Jury Subpoenas*, 318 F.3d 379, 381-82 (2d Cir. 2003) (noting that foreign country's response to MLAT request was still incomplete after two years); *United States v. Safavian*, 644 F. Supp. 2d 1, 14 n.5 (D.D.C. 2009) (noting the long "length of time that frequently is required to acquire evidence by way of an MLAT"). It is no accident that

---

<sup>26</sup> While Ireland has said that it would "consider, as expeditiously as possible, a request" for assistance under the MLAT, it has not confirmed that it would provide the information sought by the Warrant pursuant to an MLAT or indicated the length of time required to provide that information. (Ireland Br. 4).

federal law specifically provides for an exclusion of time under the Speedy Trial Act (for up to a year), as well as the suspension of a criminal statute of limitations (for up to three years), while the government is waiting to receive foreign evidence in response to an MLAT request. *See* 18 U.S.C. §§ 3161(h)(8) & 3292.

While Microsoft faults the District Court for giving undue weight to the negative effects Microsoft's construction of the SCA would have on the investigation and prosecution of criminals (Br. 59), that very real concern is fully entitled to the weight it received below. Email and other electronic communications are used extensively by criminals of all types in the United States and abroad, from fraudsters to hackers to drug dealers, in furtherance of violations of U.S. law. The ability to obtain electronically stored information from domestic service providers—pursuant to judicial authorization as required by the SCA—is a fundamental component of effective modern law enforcement. Yet such information, like the data sought by the Warrant here, can be maintained in any location and moved around the world easily, at any time and for any reason. Were Microsoft's position adopted, the government's ability to obtain such information from a provider would turn entirely on whether it happens to be stored here or abroad, even though the provider, based in the United States, maintains continuing control over the data wherever it may be stored at any given time. Such a regime would be rife with potential for arbitrary outcomes and criminal abuse.

Microsoft's own data storage policy provides but one illustration. According to Microsoft, where a user's data is stored depends entirely on which country the user selects when signing up for the account. Microsoft does not require or verify any actual connection between the user and the selected country. There is no good reason to believe, and Microsoft offers none, that Congress intended to leave it up to the whim of the provider, or the vagaries of its data storage practices, whether evidence should be disclosed to law enforcement. It is even less likely that Congress intended to create a readily manipulated loophole to the disclosure requirements it created. As the District Court cautioned, a criminal user could easily manipulate Microsoft's storage policy to evade the reach of U.S. law enforcement (at least under Microsoft's reading of the statute) "by the simple expedient of giving false residence information, thereby causing the [provider] to assign his account to a server outside the United States." *In re Warrant to Search a Certain E-Mail Account*, 15 F. Supp. 3d at 474. Microsoft's construction of the SCA cuts a gaping hole in the SCA's disclosure regime that would be easily exploited by criminals, both domestic and foreign.

Nor would any legitimate privacy interests be furthered by placing these records beyond the government's reach. When the government obtains an SCA warrant, it means that a neutral magistrate has determined, on a probable cause standard, that evidence of a crime likely resides in the relevant electronic data. The requirement of prior judicial authorization based on a probable cause finding fully vindicates any privacy rights attached to that data. In-

deed, Microsoft has previously conceded that any “concerns in the United States about an invasion of privacy are addressed” by the SCA’s warrant requirement. (A. 271-72).

Microsoft’s concession that privacy interests have been protected by the Warrant in this case is well-founded, because the balance struck by the SCA between protecting user privacy and facilitating criminal investigations is precisely the one recently recognized by the Supreme Court in *Riley v. California*, 134 S. Ct. 2473 (2014). There, the Court held that the police could not search incident to arrest a suspect’s mobile telephone because “[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals.” *Riley v. California*, 134 S. Ct. at 2485. Microsoft embraces that ruling, citing it throughout its brief, but the Supreme Court did not place the content of cell phones beyond the reach of law enforcement in the way that Microsoft endeavors to do here with respect to emails stored abroad. To the contrary, the Court imposed the time-tested protection of a warrant based on probable cause. *See id.* at 2493 (“Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.”). A warrant based on probable cause is precisely what the Government obtained here and served on Microsoft to obtain the contents of the Account. It is the gold standard for protecting civil liberties.

Microsoft and amici also ask this Court to excuse compliance with the Warrant because the long-standing practice of compelling disclosure of records supposedly threatens the “information technology sector’s continued ability to operate and compete globally.” (Br. 59; BSA Br. 11-14). Microsoft is not the first corporation (and is unlikely to be the last) to “paint[] a dismal picture of foreign companies boycotting American” companies because of an order compelling the disclosure of records stored abroad. *First Nat. City Bank*, 396 F.2d at 904. But, as this Court has previously recognized, even if those fears have a basis in reality, “the protection of the foreign economic interests of the United States must be left to the appropriate departments of our government,” not the courts.<sup>27</sup> *Id.* Equally unavailing is Microsoft’s concern that, even under the balancing of interests authorized by this Court’s precedents, it might still be “caught in the middle of a conflict” of laws. (Br. 60 (internal quotation marks omitted)). This Court and others have rejected such arguments—even where, unlike here, they are based on more than mere speculation. *See, e.g., First Nat. City Bank v. I.R.S.*, 271 F.2d at 620 (“If the Bank cannot, as it were, serve two

---

<sup>27</sup> There is good reason to doubt that these fears have a basis in reality in light of the SCA’s warrant requirement, which is specifically designed to protect legitimate privacy interests by requiring that any intrusion on those interests be properly justified by the need to uncover evidence of a crime. This is hardly an unchecked exercise of power.



masters and comply with the lawful requirements both of the United States and of Panama, perhaps it should surrender to one sovereign or the other the privileges received therefrom.”); *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d at 828 (“[T]his court simply cannot acquiesce in the proposition that United States criminal investigations must be thwarted whenever there is conflict with the interest of other states.”).

Whether compliance with the SCA will have any negative effect on Microsoft’s business, or that of any other service provider, is purely speculative and outweighed by powerful government interests. The fact remains that there exists probable cause to believe that evidence of a violation of U.S. criminal law, affecting U.S. residents and implicating U.S. interests, is present in records under Microsoft’s control. Microsoft is a U.S.-based company, enjoying all the rights and privileges of doing business in this country. With the benefits of corporate citizenship in the United States come corresponding responsibilities, including the responsibility to comply with a disclosure order issued by a U.S. court. Microsoft should not be heard to complain that doing so might harm its bottom line. The production of evidence in response to legal process “is not to be regarded as a gratuity, or a courtesy, or an ill-required favor. It is a duty not to be grudged or evaded.” *Kaufman v. Edelstein*, 539 F.2d 811, 820 (2d Cir. 1976) (quoting *Wigmore on Evidence* § 2192 at 72 (1961)).

**CONCLUSION**

**The orders of the District Court should be affirmed.**

Dated: New York, New York  
March 9, 2015

Respectfully submitted,

PREET BHARARA,  
*United States Attorney for the  
Southern District of New York,  
Attorney for the United States  
of America.*

JUSTIN ANDERSON,  
SERRIN TURNER,  
*Assistant United States Attorneys,  
Of Counsel.*

**CERTIFICATE OF COMPLIANCE**

Pursuant to Rule 32(a)(7)(C) of the Federal Rules of Appellate Procedure, the undersigned counsel hereby certifies that this brief complies with the type-volume limitation of Rule 32(a)(7)(B). As measured by the word processing system used to prepare this brief, there are 13,714 words in this brief.

PREET BHARARA,  
*United States Attorney for the  
Southern District of New York*

By: JUSTIN ANDERSON,  
*Assistant United States Attorney*

**ADDENDUM**

Add. 1

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

14 MAG [REDACTED]

In the Matter of a Warrant for Content  
and Other Information Associated with  
the Email Account

[REDACTED]@FLASH.NET Maintained  
at Premises Controlled by [REDACTED]  
Internet Services, USAO Reference  
No. 2014R [REDACTED]

**SEARCH WARRANT**

TO: [REDACTED] Internet Services ("Provider")

United States Postal Inspections Service ("Investigative Agency")

**1. Warrant.** Upon an affidavit of Postal Inspector [REDACTED] of the United States Postal Inspections Service, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [REDACTED]@FLASH.NET, maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance.

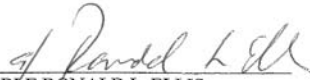
Add. 2

The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

Dated: New York, New York

11/19/14  
Date Issued

12:16<sup>0</sup> PM  
Time Issued

  
\_\_\_\_\_  
HONORABLE RONALD L. ELLIS  
United States Magistrate Judge  
Southern District of New York

Add. 3

**Email Search Attachment A**

**I. Subject Account and Execution of Warrant**

This warrant is directed to [REDACTED] Internet Services (the "Provider"), headquartered at [REDACTED] Morrisville, NC 27560, and applies to all content and other information within the Provider's possession, custody, or control associated with the email account [REDACTED]@FLASH.NET (the "Subject Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

**II. Information to be Produced by the Provider**

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email), limited to items sent, received, or created between August 2011 and September 2014.

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone

Add. 4

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

**III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of mail and wire fraud, in violation of Title 18, United States Code, Section 1341 and 1343, including the following:

a. Evidence of criminal conduct involving fraudulent misrepresentations concerning

[REDACTED] by the user of the Subject Account such as [REDACTED]  
[REDACTED]  
[REDACTED]

b. [REDACTED]

[REDACTED]  
[REDACTED]



Add. 5

c. The identity of co-conspirators and/or victims of the fraudulent criminal activity as identified by email communications between the user of the Subject Account and such individuals; and

d. Emails showing the length of time and time period during which mail or wire fraud activity was undertaken by the user of the Subject Account and others.

In conducting the search authorized by the Search Warrant, the government shall make reasonable efforts to utilize computer search methodology to search only for files, documents or other electronically stored information which are identified in the Search Warrant itself. [REDACTED]

[REDACTED]