United States Court of Appeals
FOR THE SECOND CIRCUIT

August Term, 2015

Argued: September 9, 2015 Decided: July 14, 2016

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.

B e f o r e :

LYNCH and CARNEY, *Circuit Judges*, and BOLDEN, *District Judge*.*

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York (1) denying Microsoft's motion to quash a warrant ("Warrant") issued under the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, to the extent that the orders required Microsoft to produce the contents of a customer's e-mail account stored on a server located outside the United States, and (2) holding Microsoft in civil contempt of court for its failure to comply with the Warrant. We

*The Honorable Victor A. Bolden, of the United States District Court for the District of Connecticut, sitting by designation.

conclude that § 2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers.

REVERSED, VACATED, AND REMANDED.

Judge Lynch concurs in a separate opinion.

E. JOSHUA ROSENKRANZ, Orrick, Herrington & Sutcliffe LLP (Robert M. Loeb and Brian P. Goldman, Orrick, Herrington & Sutcliffe LLP, New York, NY; Guy Petrillo, Petrillo Klein & Boxer LLP, New York, NY; James M. Garland and Alexander A. Berengaut, Covington & Burling LLP, Washington, DC; Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer, and Nathaniel Jones, Microsoft Corp., Redmond, WA; *on the brief*), *for Microsoft Corporation*.

JUSTIN ANDERSON, Assistant United States Attorney (Serrin Turner, Assistant United States Attorney, *on the brief*), *for* Preet Bharara, United States Attorney for the Southern District of New York, New York, NY.

Brett J. Williamson, David K. Lukmire, Nate Asher, O'Melveny & Myers LLP, New York, NY; Faiza Patel, Michael Price, Brennan Center for Justice, New York, NY; Hanni Fakhoury, Electronic Frontier Foundation, San Francisco, CA; Alex Abdo, American Civil Liberties Union Foundation, New York, NY; *for Amici Curiae* Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation, *in support of Appellant*.

Kenneth M. Dreifach, Marc J. Zwillinger, Zwillgen PLLC, New York, NY and Washington, DC, *for Amicus Curiae* Apple, Inc., *in support of Appellant*.

Andrew J. Pincus, Paul W. Hughes, James F. Tierney, Mayer Brown LLP, Washington, DC, *for Amici Curiae* BSA | The Software Alliance, Center for Democracy and Technology, Chamber of Commerce of the United States, The National Association of Manufacturers, and ACT | The App Association, *in support of Appellant*.

Steven A. Engel, Dechert LLP, New York, NY, *for Amicus Curiae* Anthony J. Colangelo, *in support of Appellant*.

Alan C. Raul, Kwaku A. Akowuah, Sidley Austin LLP, Washington, DC, *for Amici Curiae* AT&T Corp., Rackspace US, Inc., Computer & Communications Industry Association, i2 Coalition, and Application Developers Alliance, *in support of Appellant*.

Peter D. Stergios, Charles D. Ray, McCarter & English, LLP, New York, NY and Hartford, CT, *for Amicus Curiae* Ireland.

Peter Karanjia, Eric J. Feder, Davis Wright Tremaine LLP, New York, NY, *for Amici Curiae* Amazon.com, Inc., and Accenture PLC, *in support of Appellant*.

Michael Vatis, Jeffrey A. Novack, Steptoe & Johnson LLP, New York, NY; Randal S. Milch, Verizon Communications Inc., New York, NY; Kristofor T. Henning, Hewlett-Packard Co., Wayne, PA; Amy Weaver, Daniel Reed, Salesforce.com, Inc., San Francisco, CA; Orin Snyder, Thomas G. Hungar, Alexander H. Southwell, Gibson, Dunn & Crutcher LLP, New York, NY; Mark Chandler, Cisco Systems, Inc., San Jose, CA; Aaron Johnson, eBay Inc., San Jose, CA, *for Amici Curiae* Verizon Communications, Inc., Cisco Systems, Inc., Hewlett-Packard Co., eBay Inc., Salesforce.com, Inc., and Infor, *in support of Appellant*.

Laura R. Handman, Alison Schary, Davis Wright Tremaine LLP, Washington, DC, *for Amici Curiae* Media Organizations, *in support of Appellant*.

Philip Warrick, Klarquist Sparkman, LLP, Portland, OR, *for Amici Curiae* Computer and Data Science Experts, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY, *for Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY; Edward McGarr, Simon McGarr, Dervila McGarr, McGarr Solicitors, Dublin, Ireland, *for Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *in support of Appellant*.

SUSAN L. CARNEY, *Circuit Judge*:

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York denying its motion to quash a warrant ("Warrant") issued under § 2703 of the Stored Communications Act ("SCA" or the "Act"), 18 U.S.C. §§ 2701 *et seq.*, and holding Microsoft in contempt of court for refusing to execute the Warrant on the government's behalf. The Warrant directed Microsoft to seize and produce the contents of an e-mail account that it maintains for a customer who uses the company's electronic communications services. A United States magistrate judge (Francis, *M.J.*) issued the Warrant on the government's application, having found probable cause to believe that the account was being used in furtherance of narcotics

trafficking. The Warrant was then served on Microsoft at its headquarters in Redmond, Washington.

Microsoft produced its customer's non-content information to the government, as directed. That data was stored in the United States. But Microsoft ascertained that, to comply fully with the Warrant, it would need to access customer content that it stores and maintains in Ireland and to import that data into the United States for delivery to federal authorities. It declined to do so. Instead, it moved to quash the Warrant. The magistrate judge, affirmed by the District Court (Preska, *C.J.*), denied the motion to quash and, in due course, the District Court held Microsoft in civil contempt for its failure.

Microsoft and the government dispute the nature and reach of the Warrant that the Act authorized and the extent of Microsoft's obligations under the instrument. For its part, Microsoft emphasizes Congress's use in the Act of the term "warrant" to identify the authorized instrument. Warrants traditionally carry territorial limitations: United States law enforcement officers may be directed by a court-issued warrant to seize items at locations in the United States and in United States-controlled areas, *see* Fed. R. Crim. P. 41(b), but their authority generally does not extend further.

The government, on the other hand, characterizes the dispute as merely about "compelled disclosure," regardless of the label appearing on the instrument. It maintains that "similar to a subpoena, [an SCA warrant] requir[es] the recipient to deliver records, physical objects, and other materials to the government" no matter where those documents are located, so long as they are subject to the recipient's custody or control. Gov't Br. at 6. It relies on a collection of court rulings construing properly-served subpoenas as imposing that broad obligation to produce without regard to a document's location. *E.g., Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983).

For the reasons that follow, we think that Microsoft has the better of the argument. When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st–century demands for access and speed and their related, evolving expectations of privacy.

Rather, in keeping with the pressing needs of the day, Congress focused on providing basic safeguards for the privacy of domestic users. Accordingly, we think it employed the term "warrant" in the Act to require pre-disclosure scrutiny of the requested search and seizure by a neutral third party, and thereby to afford heightened privacy protection in the United States. It did not abandon the instrument's territorial limitations and other constitutional requirements. The application of the Act that the government proposes — interpreting "warrant" to require a service provider to retrieve material from beyond the borders of the United States —would require us to disregard the presumption against extraterritoriality that the Supreme Court re-stated and emphasized in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010) and, just recently, in *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, 2016 WL 3369423 (June 20, 2016). We are not at liberty to do so.

We therefore decide that the District Court lacked authority to enforce the Warrant against Microsoft. Because Microsoft has complied with the Warrant's domestic directives and resisted only its extraterritorial aspects, we REVERSE the District Court's denial of Microsoft's motion to quash, VACATE its finding of civil contempt, and REMAND the cause with instructions to the District Court to quash the

Warrant insofar as it directs Microsoft to collect, import, and produce to the government customer content stored outside the United States.

BACKGROUND

I. Microsoft's Web-Based E-mail Service

The factual setting in which this dispute arose is largely undisputed and is established primarily by affidavits submitted by or on behalf of the parties.

Microsoft Corporation is a United States business incorporated and headquartered in Washington State. Since 1997, Microsoft has operated a "web-based e-mail" service available for public use without charge. Joint Appendix ("J.A.") at 35. It calls the most recent iteration of this service Outlook.com.[1] The service allows Microsoft customers to send and receive correspondence using e-mail accounts hosted by the company. In a protocol now broadly familiar to the ordinary citizen, a customer uses a computer to navigate to the Outlook.com web address, and there, after logging in with username and password, conducts correspondence electronically.

Microsoft explains that, when it provides customers with web-based access to e-mail accounts, it stores the contents of each user's e-mails, along with a variety of non-content information related to the account and to the account's e-mail traffic, on a network of servers.[2] The company's servers are housed in datacenters operated by it and its subsidiaries.[3]

---

[1] The company inaugurated Outlook.com in 2013 as a successor to Microsoft's earlier Hotmail.com and MSN.com services.

[2] A "server" is "a shared computer on a network that provides services to clients. . . . An Internet-connected web server is [a] common example of a server." Harry Newton & Steve Schoen, Newton's Telecom Dictionary 1084 (28th ed. 2014) ("*Newton's Telecom Dictionary*").

[3] A "datacenter" is "[a] centralized location where computing resources (*e.g.* host computers, servers, peripherals, applications, databases, and network access) critical to an organization are maintained in a highly controlled physical environment (temperature, humidity, etc.)."

Microsoft currently makes "enterprise cloud service offerings" available to customers in over 100 countries through Microsoft's "public cloud."[4] The service offerings are "segmented into regions, and most customer data (*e.g.* email, calendar entries, and documents) is generally contained entirely within one or more data centers in the region in which the customer is located." J.A. at 109. Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when subscribing to the service. Microsoft does so, it explains, "in part to reduce 'network latency'"[5]—*i.e.*, delay—inherent in web-based computing services and thereby to improve the user's experience of its service. J.A. at 36–37. As of 2014, Microsoft "manage[d] over one million server computers in [its] datacenters worldwide, in over 100 discrete leased and owned datacenter facilities, spread over 40 countries." *Id.* at 109. These facilities, it avers, "host more than 200 online services, used by over 1 billion customers and over 20 million businesses worldwide." *Id.* at 109.

One of Microsoft's datacenters is located in Dublin, Ireland, where it is operated by a wholly owned Microsoft subsidiary. According to Microsoft, when its system automatically determines, "based on [the user's] country code," that storage for an e-mail account "should be migrated to the Dublin datacenter," it transfers the data associated with the account to that location. *Id.* at 37. Before making the transfer, it

---

Newton's Telecom Dictionary at 373.

[4] The Supreme Court has recently described "[c]loud computing" as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

[5] Microsoft explains network latency as "the principle of network architecture that the greater the geographical distance between a user and the datacenter where the user's data is stored, the slower the service." J.A. at 36.

does not verify user identity or location; it simply takes the user-provided information at face value, and its systems migrate the data according to company protocol.

Under practices in place at the time of these proceedings, once the transfer is complete, Microsoft deletes from its U.S.-based servers "all content and non-content information associated with the account in the United States," retaining only three data sets in its U.S. facilities. *Id*. at 37. First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality control purposes." *Id.* Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database. *Id.* at 37–38**.**

Microsoft asserts that, after the migration is complete, the "only way to access" user data stored in Dublin and associated with one of its customer's web-based e-mail accounts is "from the Dublin datacenter." *Id*. at 37. Although the assertion might be read to imply that a Microsoft employee must be physically present in Ireland to access the user data stored there, this is not so. Microsoft acknowledges that, by using a database management program that can be accessed at some of its offices in the United States, it can "collect" account data that is stored on any of its servers globally and bring that data into the United States. *Id*. at 39–40.

II. Procedural History

On December 4, 2013, Magistrate Judge James C. Francis IV of the United States District Court for the Southern District of New York issued the "Search and Seizure Warrant" that became the subject of Microsoft's motion to quash.

Although the Warrant was served on Microsoft, its printed boilerplate language advises that it is addressed to "[a]ny authorized law enforcement officer." *Id*. at 44. It commands the recipient to search "[t]he PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation."[6] *Id*. It requires the "officer executing [the] warrant, or an officer present during the execution of the warrant" to "prepare an inventory . . . and promptly return [the] warrant and inventory to the Clerk of the Court." *Id.*

Its Attachment A, "Property To Be Searched," provides, "This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation . . . ." *Id*. at 45. Attachment C, "Particular Things To Be Seized,"[7] directs Microsoft to disclose to the government, "for the period of inception of the account to the present," and "[t]o the extent that the information . . . is within the possession, custody, or control of MSN [redacted]," *id*., the following information:

> (a) "The contents of all e-mails stored in the account, including copies of e-mails sent from the account";
> (b) "All records or other information regarding the identification of the account," including, among other things, the name, physical address, telephone numbers, session times and durations, log-in IP addresses, and sources of payment associated with the account;
> (c) "All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files"; and
> (d) "All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken."

---

[6] The name of the e-mail address associated with the account is subject to a sealing order and does not bear on our analysis.

[7] Although the Warrant includes an Attachment A and C, it appears to have no Attachment B.

J.A. 46–47. [8]

After being served with the Warrant, Microsoft determined that the e-mail contents stored in the account were located in its Dublin datacenter. Microsoft disclosed all other responsive information, which was kept within the United States, and moved the magistrate judge to quash the Warrant with respect to the user content stored in Dublin.

As we have recounted, the magistrate judge denied Microsoft's motion to quash. In a Memorandum and Order, he concluded that the SCA authorized the District Court to issue a warrant for "information that is stored on servers abroad." *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) ("*In re Warrant*"). He observed that he had found probable cause for the requested search, and that the Warrant was properly served on Microsoft in the United States. He noted that, inasmuch as an SCA warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the ISP [Internet service provider] to search its servers and seize the e-mail account in question." *Id.* at 471. Accordingly, he determined that Congress intended in the Act's warrant provisions to import obligations similar to those associated with a subpoena to "produce information in its possession, custody, or control regardless of the location of that information." *Id.* at 472 (citing *Marc Rich*, 707 F.2d at 667). While acknowledging that Microsoft's analysis in favor of quashing the Warrant with respect to foreign-stored customer content was "not inconsistent with the statutory language," he saw Microsoft's position as "undermined by the structure of the SCA, its legislative history,"

[8] The Warrant also describes in Attachment C techniques that would be used (presumably by the government, not Microsoft) "to search the seized e-mails for evidence of the specified crime." J.A. at 47.

and "by the practical consequences that would flow from adopting it." He therefore concluded that Microsoft was obligated to produce the customer's content, wherever it might be stored. He also treated the place where the government would *review* the content (the United States), not the place of *storage* (Ireland), as the relevant place of seizure.

Microsoft appealed the magistrate judge's decision to Chief Judge Loretta A. Preska, who, on *de novo* review and after a hearing, adopted the magistrate judge's reasoning and affirmed his ruling from the bench. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 1:13-mj-02814 (S.D.N.Y. filed Dec. 4, 2013), ECF No. 80 (order reflecting ruling made at oral argument).

Microsoft timely noticed its appeal of the District Court's decision denying the motion to quash. Not long after, the District Court acted on a stipulation submitted jointly by the parties and held Microsoft in civil contempt for refusing to comply fully with the Warrant.[9] *Id.* at ECF No. 92. Microsoft timely amended its notice of appeal to reflect its additional challenge to the District Court's contempt ruling.

We now reverse the District Court's denial of Microsoft's motion to quash; vacate the finding of contempt; and remand the case to the District Court with instructions to

[9] As reflected in their stipulation, Microsoft and the government agreed to the contempt finding to ensure our Court's appellate jurisdiction over their dispute. *See United States v. Punn*, 737 F.3d 1, 5 (2d Cir. 2013) (noting general rule that contempt finding needed before ruling denying motion to quash is sufficiently "final" to support appellate jurisdiction). Because Microsoft timely appealed the contempt ruling, we need not decide whether we would have had jurisdiction over an appeal taken directly from the denial of the motion to quash. *See United States v. Constr. Prods. Research, Inc.*, 73 F.3d 464, 468–69 (2d Cir. 1996) (noting exception to contempt requirement as basis for appellate jurisdiction in context of third party subpoena issued in administrative investigation).

quash the Warrant insofar as it calls for production of customer content stored outside the United States.

III. Statutory Background

The Warrant was issued under the provisions of the Stored Communications Act, legislation enacted as Title II of the Electronic Communications Privacy Act of 1986. Before we begin our analysis, some background will be useful.

A. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act ("ECPA") became law in 1986.[10] As it is summarized by the Department of Justice, ECPA "updated the Federal Wiretap Act of 1968, which addressed interception of conversations using 'hard' telephone lines, but did not apply to interception of computer and other digital and electronic communications."[11] ECPA's Title II is also called the Stored Communications Act ("SCA"). The Act "protects the privacy of the contents of files stored by service

---

[10] Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848, 1848–73 (1986) (codified as amended at 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701 *et seq.*, and 18 U.S.C. §§ 3121 *et seq.*).

[11] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last visited May 12, 2016). The Department advises that the acronym "ECPA" is commonly used to refer to the three titles of ECPA as a group (Titles I, II, and III of Pub. L. 99-508). *Id.* Title I "prohibits the intentional actual or attempted interception, use, disclosure, or procurement of any other person" to intercept wire, oral, or electronic transmissions; Title II is the Stored Communications Act, discussed in the text; Title III "addresses pen register and trap and trace devices," requiring government entities to obtain a court order authorizing their installation. *Id.* Title I and III are codified at 18 U.S.C. §§ 2510-22; Title II is codified at 18 U.S.C. §§ 2701-12, and constitutes chapter 121 of Title 18.

providers and of records held about the subscriber by service providers," according to the Justice Department.[12] We discuss its provisions further below.

B. The Technological Setting in 1986

When it passed the Stored Communications Act almost thirty years ago, Congress had as reference a technological context very different from today's Internet-saturated reality. This context affects our construction of the statute now.

One historian of the Internet has observed that "before 1988, the *New York Times* mentioned the Internet only once—in a brief aside." Roy Rosenzweig, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*, 103 Am. Hist. Rev. 1530, 1530 (1998). The TCP/IP data transfer protocol—today, the standard for online communication—began to be used by the Department of Defense in about 1980. *See* Leonard Kleinrock, *An Early History of the Internet*, IEEE Commc'ns Mag. 26, 35 (Aug. 2010). The World Wide Web was not created until 1990, and we did not even begin calling it that until 1993. Daniel B. Garrie & Francis M. Allegra, *Plugged In: Guidebook to Software and the Law* § 3.2 (2015 ed.). Thus, a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future when Congress first took action to protect user privacy. *See* Craig Partridge, *The Technical Development of Internet Email*, IEEE Annals of the Hist. of Computing 3, 4 (Apr.-June 2008).

C. The Stored Communications Act

As the government has acknowledged in this litigation, "[t]he SCA was enacted to extend to electronic records privacy protections analogous to those provided by the

[12] *See supra* note 11.

Fourth Amendment." Gov't Br. at 29 (citing S. Comm. on Judiciary, Electronic Communications Privacy Act of 1986, S. Rep. No. 99-541, at 5 (1986)). The SCA provides privacy protection for users of two types of electronic services—electronic communication services ("ECS") and remote computing services ("RCS")—then probably more distinguishable than now.[13] *See* 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, 1213–14 (2004). An ECS generally operated by providing the user access to a central computer system through which to send electronic messages over telephone lines. S. Rep. No. 99-541, at 8. If the intended recipient also subscribed to the service, the provider temporarily stored the message in the recipient's electronic "mail box" until the recipient "call[ed] the company to retrieve its mail." *Id.* If the intended recipient was not a subscriber, the service provider could print the communication on paper and complete delivery by postal service or courier. *Id.*; U.S. Congress, Office of Technology Assessment, OTA-CIT-293, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 47–48 (1985).[14] An RCS generally operated either by providing customers with access to computer processing facilities in a "time-sharing arrangement," or by directly processing data that a customer transmitted electronically to the provider by means of electronic communications, and transmitting back the requested results of particular operations. S. Rep. No. 99-541, at 10–11. We will refer to

---

[13] *See* 18 U.S.C. § 2510(15) (in ECPA Title I, defining "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); § 2711(2) (in ECPA Title II, the SCA, defining "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

[14] For example, in 1984, Federal Express entered the e-mail market with a service that provided for two-hour delivery of facsimile copies of e-mail messages up to five pages in length. U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, at 47.

Microsoft and other providers of ECS and RCS jointly as "service providers," except where the distinction makes a difference.

As to both services, the Act imposes general obligations of non-disclosure on service providers and creates several exceptions to those obligations. Thus, its initial provision, § 2701, prohibits unauthorized third parties from, among other things, obtaining or altering electronic communications stored by an ECS, and imposes criminal penalties for its violation. Section 2702 restricts the circumstances in which service providers may disclose information associated with and contents of stored communications to listed exceptions, such as with the consent of the originator or upon notice to the intended recipient, or pursuant to § 2703. Section 2703 then establishes conditions under which the government may require a service provider to disclose the contents of stored communications and related obligations to notify a customer whose material has been accessed. Section 2707 authorizes civil actions by entities aggrieved by violations of the Act, and makes "good faith reliance" on a court warrant or order "a complete defense." 18 U.S.C. § 2707(e).[15]

Regarding governmental access in particular, § 2703 sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government. Basic subscriber and transactional information can be obtained simply with an administrative subpoena.[16] 18 U.S.C. § 2703(c)(2). Other

[15] Other provisions of the Act address, among other things, preservation of backup data (§ 2704); delaying notice to a customer whose information has been accessed (§ 2705); cost reimbursement for assembling data demanded under the Act (§ 2706); and exclusivity of remedies that the Act provides to a person aggrieved by its violation (§ 2708).

[16] An "administrative subpoena" is "a subpoena issued by an administrative agency to compel an individual to provide information to the agency." *Administrative subpoena*, Black's Law Dictionary (10th ed. 2014). To obtain such a subpoena, the government need not demonstrate probable cause. *See EEOC v. United Parcel Serv., Inc.*, 587 F.3d 136, 139-40 (2d Cir. 2009).

non-content records can be obtained by a court order (a "§ 2703(d) order"), which may be issued only upon a statement of "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation." § 2703(c)(2), (d). The government may also obtain some user content with an administrative subpoena or a § 2703(d) order, but only if notice is provided to the service provider's subscriber or customer. § 2703(b)(1)(B). To obtain "priority stored communications" (our phrase), as described below, the Act generally requires that the government first secure a warrant that has been issued "using the procedures described in the Federal Rules of Criminal Procedure," or using State warrant procedures, both of which require a showing of probable cause.[17] Priority stored communications fall into two categories: For

[17] Thus, § 2703, "Required disclosure of customer communications or records," provides in part as follows:

> (a) Contents of wire or electronic communications in electronic storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.
>
> (b) Contents of wire or electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

electronic communications stored *recently* (that is, for less than 180 days) by an ECS, the government *must* obtain a warrant. § 2703(a). For older electronic communications and those held by an RCS, a warrant is also required, unless the Government is willing to provide notice to the subscriber or customer. § 2703(b)(1)(A).

As noted, § 2703 calls for those warrants issued under its purview by federal courts to be "issued using the procedures described in the Federal Rules of Criminal Procedure." Rule 41 of the Federal Rules of Criminal Procedure, entitled "Search and Seizure," addresses federal warrants. It directs "the magistrate judge or a judge of a state court of record" to issue the warrant to "an officer authorized to execute it." Rule 41(e)(1). And insofar as territorial reach is concerned, Rule 41(b) describes the extent of

---

> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
>
> > (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
> >
> > (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title. . . .
>
> (g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

the power of various authorities (primarily United States magistrate judges) to issue warrants with respect to persons or property located within a particular federal judicial district. It also allows magistrate judges to issue warrants that may be executed outside of the issuing district, but within another district of the United States. Fed. R. Crim. P. 41(b)(2), (b)(3). Rule 41(b)(5) generally restricts the geographical reach of a warrant's execution, if not in another federal district, to "a United States territory, possession, or commonwealth," and various diplomatic or consular missions of the United States or diplomatic residences of the United States located in a foreign state.

DISCUSSION

I. Standard of Review

We will vacate a finding of civil contempt that rests on a party's refusal to comply with a court order if we determine that the district court relied on a mistaken understanding of the law in issuing its order. *United States ex rel. Touhy v. Ragen*, 340 U.S. 462, 464–70 (1951). Similarly, we will vacate a district court's denial of a motion to quash if we conclude that the denial rested on a mistake of law.[18] *See In re Subpoena Issued to Dennis Friedman*, 350 F.3d 65, 68–69 (2d Cir. 2003).

It is on the legal predicate for the District Court's rulings—its analysis of the Stored Communications Act, in particular, and of the principles of construction set forth by the Supreme Court in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010)—that we focus our attention in this appeal.

---

[18] Our Court has not squarely held what standard governs our review of a district court's denial of a motion to quash and its related contempt finding. We need not dwell long on this threshold question, however, because even a deferential abuse-of-discretion review incorporates a *de novo* examination of the district court's rulings of law, such as we conduct here. *See, e.g., In re Grand Jury Subpoena Issued June 18, 2009*, 593 F.3d 155, 157 (2d Cir. 2010).

II. Whether the SCA Authorizes Enforcement of the Warrant as to Customer Content Stored in Ireland

A. Analytic Framework

The parties stand far apart in the analytic frameworks that they present as governing this case.

Adopting the government's view, the magistrate judge denied Microsoft's motion to quash, resting on the legal conclusion that an SCA warrant is more akin to a subpoena than a warrant, and that a properly served subpoena would compel production of any material, including customer content, so long as it is stored at premises "owned, maintained, controlled, or operated by Microsoft Corporation." *In re Warrant*, 15 F. Supp. 3d at 468 (quoting Warrant). The fact that those premises were located abroad was, in the magistrate judge's view, of no moment. *Id.* at 472.

Microsoft offers a different conception of the reach of an SCA warrant. It understands such a warrant as more closely resembling a traditional warrant than a subpoena. In its view, a warrant issued under the Act cannot be given effect as to materials stored beyond United States borders, regardless of what may be retrieved electronically from the United States and where the data would be reviewed. To enforce the Warrant as the government proposes would effect an unlawful extraterritorial application of the SCA, it asserts, and would work an unlawful intrusion on the privacy of Microsoft's customer.

Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States. As to the citizenship of the customer whose

e-mail content was sought, the record is silent. For its part, the SCA is silent as to the reach of the statute as a whole and as to the reach of its warrant provisions in particular. Finally, the presumption against extraterritorial application of United States statutes is strong and binding. *See Morrison*, 561 U.S. at 255. In these circumstances, we believe we must begin our analysis with an inquiry into whether Congress, in enacting the warrant provisions of the SCA, envisioned and intended those provisions to reach outside of the United States. If we discern that it did not, we must assess whether the enforcement of this Warrant constitutes an unlawful extraterritorial application of the statute. We thus begin with a brief review of *Morrison*, which outlines the operative principles.

B. *Morrison* and the Presumption Against Extraterritoriality

When interpreting the laws of the United States, we presume that legislation of Congress "is meant to apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. *Id*. at 255 (internal quotation marks omitted); *see also RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, __, 2016 WL 3369423, at *7 (June 20, 2016). This presumption rests on the perception that "Congress ordinarily legislates with respect to domestic, not foreign matters." *Id*. The presumption reflects that Congress, rather than the courts, has the "facilities necessary" to make policy decisions in the "delicate field of international relations." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (quoting *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)). In line with this recognition, the presumption is applied to protect against "unintended clashes between our laws and those of other nations which could result in international discord." *Equal Emp't Opportunity Comm'n v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991) ("*Aramco*"); s*ee generally Park Central Global Hub Ltd. v. Porsche Auto. Holdings SE*, 763 F.3d 198 (2d Cir. 2014) (per curiam).

To decide whether the presumption limits the reach of a statutory provision in a particular case, "we look to see whether 'language in the [relevant Act] gives any indication of a congressional purpose to extend its coverage beyond places over which the United States has sovereignty or has some measure of legislative control.'" *Aramco*, 499 U.S. at 248 (alteration in original) (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949)). The statutory provision must contain a "clear indication of an extraterritorial application"; otherwise, "it has none." *Morrison*, 561 U.S. at 255; *see also RJR Nabisco*, 579 U.S. at __, 2016 WL 3369423, at *7.

Following the approach set forth in *Morrison*, our inquiry proceeds in two parts. We first determine whether the relevant statutory provisions contemplate extraterritorial application. *Id*. at 261–65. If we conclude that they do not, by identifying the statute's focus and looking at the facts presented through that prism, we then assess whether the challenged application is "extraterritorial" and therefore outside the statutory bounds. *Id.* at 266–70.

C. Whether the SCA's Warrant Provisions Contemplate Extraterritorial Application

We dispose of the first question with relative ease. The government conceded at oral argument that the warrant provisions of the SCA do not contemplate or permit extraterritorial application.[19] Our review of the statute confirms the soundness of this concession.

[19] When asked, "What text in the Stored Communications Act do you point to, to support your assertion that . . . Congress intended extraterritorial application?", the government responded, "There's no extraterritorial application here at all." Recording of Oral Argument at 1:06:40–1:07:00. Later, when Judge Lynch observed, "I take it that suggests that the government actually agrees that there shall not be extraterritorial application of the Stored Communications Act . . . what this dispute is about is about the focus of the statute and what counts as an extraterritorial

1. Plain Meaning of the SCA

As observed above, the SCA permits the government to require service providers to produce the contents of certain priority stored communications "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703(a), (b)(1)(a). The provisions in § 2703 that permit a service provider's disclosure in response to a duly obtained warrant do not mention any extraterritorial application, and the government points to no provision that even implicitly alludes to any such application. No relevant definition provided by either Title I or Title II of ECPA, *see* 18 U.S.C. §§ 2510, 2711, suggests that Congress envisioned any extraterritorial use for the statute.

When Congress intends a law to apply extraterritorially, it gives an "affirmative indication" of that intent. *Morrison*, 561 U.S. at 265. It did so, for example, in the statutes at issue in *Weiss v. National Westminster Bank PLC*, 768 F.3d 202, 207 & n.5 (2d Cir. 2014) (concluding that definition of "international terrorism" within 18 U.S.C. § 2331(1) covers extraterritorial conduct because Congress referred to acts that "occur primarily outside the territorial jurisdiction of the United States") and *United States v. Weingarten*, 632 F.3d 60, 65 (2d Cir. 2011) (concluding that 18 U.S.C. § 2423(b) applies to extraterritorial conduct because it criminalizes "travel in foreign commerce undertaken with the intent to commit sexual acts with minors" that would violate United States law had the acts occurred in the jurisdiction of the United States). We see no such indication in the SCA.

---

application of the statute," the government answered, "That's right, Judge." *Id*. at 1:25:38–1:26:05.

We emphasize further that under § 2703, any "court of competent jurisdiction"—defined in § 2711(3)(B) to include "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants"—may issue an SCA warrant. Section 2703(a) refers directly to the use of State warrant procedures as an adequate basis for issuance of an SCA warrant. 18 U.S.C. § 2703(a). We think it particularly unlikely that, if Congress intended SCA warrants to apply extraterritorially, it would provide for such far-reaching state court authority without at least "address[ing] the subject of conflicts with foreign laws and procedures." *Aramco*, 499 U.S. at 256; *see also American Ins. Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003) (describing as beyond dispute the notion that "state power that touches on foreign relations must yield to the National Government's policy").

The government asserts that "[n]othing in the SCA's text, structure, purpose, or legislative history indicates that compelled production of records is *limited* to those stored domestically." Gov't Br. at 26 (formatting altered and emphasis added). It emphasizes the requirement placed on a service provider to disclose customers' data, and the absence of any territorial reference restricting that obligation. We find this argument unpersuasive: It stands the presumption against extraterritoriality on its head. It further reads into the Act an extraterritorial awareness and intention that strike us as anachronistic, and for which we see, and the government points to, no textual or documentary support.[20]

[20] Seeking additional grounds for its position that to apply *Morrison* in this case is to proceed on a false premise, the government argues that the presumption against extraterritoriality applies only to "substantive provisions" of United States law, and that the SCA's warrant provisions are procedural. Gov't Br. at 31. The proposition that the SCA's protections are merely procedural might reasonably be questioned. But even assuming that they are procedural, the government gains no traction with this argument, which we rejected in *Loginovskaya v. Batratchenko*, 764 F.3d 266, 272-73 (2d Cir. 2014).

2. The SCA's Use of the Term of Art "Warrant"

Congress's use of the term of art "warrant" also emphasizes the domestic boundaries of the Act in these circumstances.

In construing statutes, we interpret a legal term of art in accordance with the term's traditional legal meaning, unless the statute contains a persuasive indication that Congress intended otherwise. *See F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012) ("[W]hen Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.'") (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)). "Warrant" is such a term of art.

The term is endowed with a legal lineage that is centuries old. The importance of the warrant as an instrument by which the power of government is exercised and constrained is reflected by its prominent appearance in the Fourth Amendment to the United States Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. It is often observed that "[t]he chief evil that prompted the framing and adoption of the Fourth Amendment was the indiscriminate searches and seizures conducted by the British under the authority of general warrants." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (internal quotation marks omitted). Warrants issued in accordance with the Fourth Amendment thus identify discrete objects and places, and restrict the government's ability to act beyond the warrant's

purview — of particular note here, outside of the place identified, which must be described in the document. *Id*. at 445–46.

As the term is used in the Constitution, a warrant is traditionally moored to privacy concepts applied within the territory of the United States: "What we know of the history of the drafting of the Fourth Amendment . . . suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters." *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 169 (2d Cir. 2008) (alteration omitted and ellipses in original) (quoting *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990)). Indeed, "if U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have dubious legal significance, if any, in a foreign nation." *Id*. at 171. Accordingly, a warrant protects privacy in a distinctly territorial way.[21]

The SCA's legislative history related to its post enactment amendments supports our conclusion that Congress intended to invoke the term "warrant" with all of its traditional, domestic connotations.[22] Since the SCA's initial passage in 1986, Congress has amended § 2703 to relax some of the Rule 41 requirements as they relate to SCA warrants. Although some address the reach of SCA warrants, none of the amendments

---

[21] The government argues that the SCA's warrant provisions were "modeled after the Right to Financial Privacy Act," 12 U.S.C. §§ 3402(3), 3406, and that the latter act also "envisions that warrants—along with subpoenas and summonses—will trigger a disclosure requirement." Gov't Br. at 19 (citing S. Rep. No. 99-541, at 3). It points to no authority definitively construing the latter act's warrant provisions, however, nor any acknowledgment in the history of the SCA that enforcement of the warrant's disclosure commands would cross international boundaries. For these reasons, we accord little weight to the observation.

[22] We note that a 2009 amendment to Rule 41 expressly authorizes the use of such warrants to seize electronically-stored data, without abandoning the requirement that the warrant specify the place from which the data is to be seized. *See* Fed. R. Crim. P. 41(e)(2)(B) (allowing magistrate judge to "authorize the seizure of *electronic storage media* or the seizure or copying of *electronically stored information*" (emphasis added)).

contradicts the term's traditional domestic limits. *See* USA PATRIOT ACT, Pub. L. 107-56, § 220; 115 Stat. 272, 291–92 (2001) (codified at 18 U.S.C. § 2703(a), (b)); 21st Century Department of Justice Appropriations Authorization Act, Pub. L. 107-273, § 11010, 116 Stat. 1758, 1822 (2002) (codified at 18 U.S.C. § 2703(g)); Foreign Evidence Request Efficiency Act of 2009, Pub. L. 111-79, § 2, 123 Stat. 2086, 2086 (2009) (codified at 18 U.S.C. § 2711(3)(A)). These amendments to the SCA are fully consistent with the historical role of warrants as legal instruments that pertain to discrete objects located within the United States, and that are designed to protect U.S. citizens' privacy interests.

The magistrate judge took a different view of the legislative history of certain amendments to the SCA. He took special notice of certain legislative history related to the 2001 amendment to the warrant provisions enacted in the USA PATRIOT ACT. A House committee report explained that "[c]urrently, Federal Rules [*sic*] of Criminal Procedure 41 requires that the 'warrant' be obtained 'within the district' where the property is located. An investigator, for example, located in Boston . . . might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California." *In re Warrant*, 15 F. Supp. 3d at 473 (quoting H.R. Rep. 107-236(I), at 57 (2001)). The magistrate judge reasoned that this statement equated the location of property with the location of the service provider, and not with the location of any server. *Id.* at 474.

But this excerpt says nothing about the need to cross international boundaries; rather, while noting the "cross-jurisdictional nature of the Internet," it discusses only amendments to Rule 41 that allow magistrate judges "within the district" to issue warrants to be executed in other "districts"—not overseas. *Id.* at 473 (quoting H.R. Rep. 107-236(I), at 58). Furthermore, the Committee discussion reflects no expectation that the material to be searched and seized would be located any place other than where the

service provider is located. Thus, the Committee's hypothetical focuses on a situation in which an investigator in Boston might seek e-mail from "an Internet service provider (ISP) *account* located in California." To our reading, the Report presumes that the service provider is located where the account is—within the United States.[23]

3. Relevance of Law on "Subpoenas"

We reject the approach, urged by the government and endorsed by the District Court, that would treat the SCA warrant as equivalent to a subpoena. The District Court characterized an SCA warrant as a "hybrid" between a traditional warrant and a subpoena because—generally unlike a warrant—it is executed by a service provider rather than a government law enforcement agent, and because it does not require the presence of an agent during its execution. *Id*. at 471; 18 U.S.C. § 2703(a)-(c), (g). As flagged earlier, the subpoena-warrant distinction is significant here because, unlike warrants, subpoenas may require the production of communications stored overseas. 15 F. Supp. 3d at 472 (citing *Marc Rich*, 707 F.2d at 667).

Warrants and subpoenas are, and have long been, distinct legal instruments.[24] Section 2703 of the SCA recognizes this distinction and, unsurprisingly, uses the

---

[23] Our brief discussion here of the law of warrants is offered in aid only of our interpretation of the statutory language. Consequently, we do not consider whether the Fourth Amendment might be understood to impose disclosure-related procedural requirements more stringent than those established by the SCA. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (finding Fourth Amendment protects certain electronic communications based on users' reasonable expectations of privacy); *see also* Email Privacy Act, H. R. 699, 114th Cong. § 3 (passed by House Apr. 27, 2016) (requiring government to obtain warrant before obtaining documents stored online).

[24] A "subpoena" (from the Latin phrase meaning "under penalty,") is "[a] writ or order commanding a person to appear before a court or other tribunal, subject to a penalty for failing to comply." *Subpoena*, Black's Law Dictionary. Relatedly, a "subpoena duces tecum" directs the person served to bring with him "specified documents, records, or things." *Subpoena duces*

"warrant" requirement to signal (and to provide) a greater level of protection to priority stored communications, and "subpoenas" to signal (and provide) a lesser level. 18 U.S.C. § 2703(a), (b)(1)(A). Section 2703 does not use the terms interchangeably. *Id.* Nor does it use the word "hybrid" to describe an SCA warrant. Indeed, § 2703 places priority stored communications entirely outside the reach of an SCA subpoena, absent compliance with the notice provisions. *Id.* The term "subpoena," therefore, stands separately in the statute, as in ordinary usage, from the term "warrant." We see no reasonable basis in the statute from which to infer that Congress used "warrant" to mean "subpoena."

Furthermore, contrary to the Government's assertion, the law of warrants has long contemplated that a private party may be required to participate in the lawful search or seizure of items belonging to the target of an investigation. When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *Gambino v. United States*, 275 U.S. 310, 316–17 (1927); *see also Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006). The SCA's warrant provisions fit comfortably within this scheme by requiring a warrant for the content of stored communications even when the warrant commands a service provider, rather than a law enforcement officer, to access the communications. 18 U.S.C. § 2703(a), (b)(1)(A), (g). Use of this mechanism does not signal that, notwithstanding its use of the term

---

tecum, Black's Law Dictionary. In contrast, a "warrant" is a "writ directing or authorizing someone to do an act [such as] one directing a law enforcer to make . . . a search, or a seizure." *Warrant*, Black's Law Dictionary. As to search warrants, the place is key: A search warrant is a "written order authorizing a law-enforcement officer to conduct a search *of a specified place*." *Search Warrant*, Black's Law Dictionary.

"warrant," Congress intended the SCA warrant procedure to function like a traditional subpoena. We see no reason to believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application.

The government nonetheless urges that the law of subpoenas relied on by the magistrate judge requires a subpoena's recipient to produce documents no matter where located, and that this aspect of subpoena law should be imported into the SCA's warrant provisions. The government argues that "subpoenas, orders, and warrants are equally empowered to obtain records . . . through a disclosure requirement directed at a service provider." Gov't Br. at 18–19. It further argues that disclosure in response to an SCA warrant should not be read to reach only U.S.-located documents, but rather all records available to the recipient. *Id*. at 26–27.

In this, the government rests on our 1983 decision in *Marc Rich*. There, we permitted a grand jury subpoena issued in a tax evasion investigation to reach the overseas business records of a defendant Swiss commodities trading corporation. The *Marc Rich* Court clarified that a defendant subject to the personal jurisdiction of a subpoena-issuing grand jury could not "resist the production of [subpoenaed] documents on the ground that the documents are located abroad." 707 F.2d at 667. The federal court had subject-matter jurisdiction over the foreign defendant's actions pursuant to the "territorial principle," which allows governments to punish an individual for acts outside their boundaries when those acts are "intended to produce and do produce detrimental effects within it." *Id.* at 666. In investigating such a case, the Court concluded, the grand jury necessarily had authority to obtain evidence related to the foreign conduct, even when that evidence was located abroad. *Id.* at 667. For that reason, as long as the Swiss corporation was subject to the grand jury's

personal jurisdiction—which the Court concluded was the case—the corporation was bound by its subpoena. *Id*. Thus, in *Marc Rich*, a subpoena could reach documents located abroad when the subpoenaed foreign defendant was being compelled to turn over its own records regarding potential illegal conduct, the effects of which were felt in the United States.

Contrary to the government's assertion, neither *Marc Rich* nor the statute gives any firm basis for importing law developed in the subpoena context into the SCA's warrant provisions. Microsoft convincingly observes that our Court has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item.[25] Appellant's Br. at 42–43. The government does not identify, and our review of this Court's precedent does not reveal, any such cases.

The government also cites, and the District Court relied on, a series of cases in which banks have been required to comply with subpoenas or discovery orders requiring disclosure of their overseas records, notwithstanding the possibility that

[25] The government contends that Microsoft has waived the argument that the government cannot compel production of records that Microsoft holds on its customers' behalf. Gov't Br. at 36 & n.14. But in the District Court proceedings, Microsoft argued that there was a "difference between, on the one hand asking a company for its own documents . . . versus when you are going after someone else's documents . . . that are entrusted to us on behalf of our clients." Transcript of Oral Argument at 17, *In re Warrant*, 1:13-mj-02814, ECF No. 93. Although this was not the centerpiece of Microsoft's argument before the District Court, it was sufficiently raised. And in any event, we are free to consider arguments made on appeal in the interests of justice even when they were not raised before the district court. *See Gibeau v. Nellis*, 18 F.3d 107, 109 (2d Cir. 1994). The government has had an ample opportunity to rebut Microsoft's position, and we see no reason to treat this important argument as beyond our consideration.

compliance would conflict with their obligations under foreign law.[26] But the Supreme Court has held that bank depositors have no protectable privacy interests in a bank's records regarding their accounts. *See United States v. Miller*, 425 U.S. 435, 440–41 (1976) (explaining that the records a bank creates from the transactions of its depositors are the bank's "business records" and not its depositors' "private papers"). Thus, our 1968 decision in *United States v. First National City Bank* poses no bar to Microsoft's argument. There, we held that a bank subject to the jurisdiction of a federal court was not absolutely entitled to withhold from a grand jury subpoena its banking records held in Frankfurt, Germany "relating to any transaction in the name of (or for the benefit of)" certain foreign customers solely because the bank faced the prospect of civil liability. 396 F.2d 897, 898, 901, 905 (2d Cir. 1968); *cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 101–02, 109 (2d Cir. 2013) (declining to issue writ of mandamus overturning district court's imposition of sanctions on foreign bank, when bank was civil defendant and refused to comply with discovery orders seeking certain foreign banking records).

We therefore conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially.

D. Discerning the "Focus" of the SCA

This conclusion does not resolve the merits of this appeal, however, because "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *Morrison*, 561 U.S. at 266. When we find that a law does

[26] Thus, in addition to *Marc Rich*, the government refers us to other cases that it characterizes as ordering production despite potential or certain conflict with the laws of other nations: *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817, 826–29 (11th Cir. 1984); *United States* v. *Vetco Inc.*, 691 F.2d 1281, 1287–91 (9th Cir. 1981); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 547, 564 (S.D.N.Y. 2002) (Chin, *J.*); *United States* v. *Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080, 1086–87 (S.D.N.Y. 1984). Gov't Br. at 16–17.

not contemplate or permit extraterritorial application, we generally must then determine whether the case at issue involves such a prohibited application. *Id* at 266–67. As we recently observed in *Mastafa v. Chevron Corp.*, "An evaluation of the presumption's application to a particular case is essentially an inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption at all." 770 F.3d 170, 182 (2d Cir. 2014).

In making this second-stage determination, we first look to the "territorial events or relationships" that are the "focus" of the relevant statutory provision. *Id*. at 183 (alterations and internal quotation marks omitted). If the domestic contacts presented by the case fall within the "focus" of the statutory provision or are "the objects of the statute's solicitude," then the application of the provision is not unlawfully extraterritorial. *Morrison*, 561 U.S. at 267. If the domestic contacts are merely secondary, however, to the statutory "focus," then the provision's application to the case is extraterritorial and precluded.

In identifying the "focus" of the SCA's warrant provisions, it is helpful to resort to the familiar tools of statutory interpretation, considering the text and plain meaning of the statute, *see, e.g., Gottlieb v. Carnival Corp.*, 436 F.3d 335, 337 (2d Cir. 2006), as well as its framework, procedural aspects, and legislative history. *Cf*. *Morrison*, 561 U.S. at 266–70 (looking to text and statutory context to discern focus of statutory provision); *Loginovskaya*, 764 F.3d at 272–73 (analyzing text, context, and precedent to discern focus for *Morrison* purposes). Having done so, we conclude that the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content — the "object[] of the statute's solicitude." *Morrison*, 561 U.S. at 267.

1. The SCA's Warrant Provisions

The reader will recall the SCA's provisions regarding the production of electronic communication content: In sum, for priority stored communications, "a governmental entity may require the disclosure . . . of the contents of a wire or electronic communication . . . only pursuant to a warrant issued using the rules described in the Federal Rules of Criminal Procedure," except (in certain cases) if notice is given to the user. 18 U.S.C. § 2703(a), (b).

In our view, the most natural reading of this language in the context of the Act suggests a legislative focus on the privacy of stored communications. Warrants under § 2703 must issue under the Federal Rules of Criminal Procedure, whose Rule 41 is undergirded by the Constitution's protections of citizens' privacy against unlawful searches and seizures. And more generally, § 2703's warrant language appears in a statute entitled the Electronic Communications Privacy Act, suggesting privacy as a key concern.

The overall effect is the embodiment of an expectation of privacy in those communications, notwithstanding the role of service providers in their transmission and storage, and the imposition of procedural restrictions on the government's (and other third party) access to priority stored communications. The circumstances in which the communications have been stored serve as a proxy for the intensity of the user's privacy interests, dictating the stringency of the procedural protection they receive—in particular whether the Act's warrant provisions, subpoena provisions, or its § 2703(d) court order provisions govern a disclosure desired by the government. Accordingly, we think it fair to conclude based on the plain meaning of the text that the privacy of the stored communications is the "object[] of the statute's solicitude," and the focus of its provisions. *Morrison*, 561 U.S. at 267.

2. Other Aspects of the Statute

In addition to the text's plain meaning, other aspects of the statute confirm its focus on privacy.

As we have noted, the first three sections of the SCA contain its major substantive provisions. These sections recognize that users of electronic communications and remote computing services hold a privacy interest in their stored electronic communications. In particular, § 2701(a) makes it unlawful to "intentionally access[] without authorization," or "intentionally exceed[] an authorization to access," a "facility through which an electronic communication service is provided" and "thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." Contrary to the government's contention, this section does more than merely protect against the disclosure of information by third parties. By prohibiting the alteration or blocking of access to stored communications, this section also shelters the communications' integrity. Section 2701 thus protects the privacy interests of users in many aspects of their stored communications from intrusion by unauthorized third parties.

Section 2702 generally prohibits providers from "knowingly divulg[ing]" the "contents" of a communication that is in electronic storage subject to certain enumerated exceptions. 18 U.S.C. § 2702(a). Sections 2701 and 2702 are linked by their parallel protections for communications that are in electronic storage. Section 2703 governs the circumstances in which information associated with stored communications may be disclosed to the government, creating the elaborate hierarchy of privacy protections that we have described.

From this statutory framework we find further reason to conclude that the SCA's focus lies primarily on the need to protect users' privacy interests. The primary obligations created by the SCA protect the electronic communications. Disclosure is permitted only as an exception to those primary obligations and is subject to conditions imposed in § 2703. Had the Act instead created, for example, a rebuttable presumption of law enforcement access to content premised on a minimal showing of legitimate interest, the government's argument that the Act's focus is on aiding law enforcement and disclosure would be stronger. *Cf. Morrison*, 561 U.S. at 267. But this is not what the Act does.

The SCA's procedural provisions further support our conclusion that the Act focuses on user privacy. As noted above, the SCA expressly adopts the procedures set forth in the Federal Rules of Criminal Procedure. 18 U.S.C. § 2703(a), (b)(1)(A). Rule 41, which governs the issuance of warrants, reflects the historical understanding of a warrant as an instrument protective of the citizenry's privacy. *See* Fed. R. Crim. P. 41. Further, the Act provides criminal penalties for breaches of those privacy interests and creates civil remedies for individuals aggrieved by a breach of their privacy that violates the Act. *See* 18 U.S.C. §§ 2701, 2707. These all buttress our sense of the Act's focus.

We find unpersuasive the government's argument, alluded to above, that the SCA's warrant provisions must be read to focus on "disclosure" rather than privacy because the SCA permits the government to obtain by mere subpoena the content of e-mails that have been held in ECS storage for *more than* 180 days. Gov't Br. at 28–29; *see* 18 U.S.C. § 2703(a). In this vein, the government submits that reading the SCA's warrant provisions to focus on the privacy of stored communications instead of disclosure would anomalously place newer e-mail content stored on foreign servers "beyond the reach of the statute entirely," while older e-mail content stored on foreign

servers could be obtained simply by subpoena, if notice is given to the user. Gov't Br. at 29. This argument assumes, however, that a subpoena issued to Microsoft under the SCA's subpoena provisions would reach a user's e-mail content stored on foreign servers. Although our Court's precedent regarding the foreign reach of subpoenas (and *Marc Rich* in particular) might suggest this result, the protections rightly accorded user content in the face of an SCA subpoena have yet to be delineated. Today, we need not determine the reach of the SCA's subpoena provisions, because we are faced here only with the lawful reach of an SCA warrant. Certainly, the service provider's role in relation to a customer's content supports the idea that persuasive distinctions might be drawn between it and other categories of subpoena recipients. *See supra* note 23.

In light of the plain meaning of the statutory language and the characteristics of other aspects of the statute, we conclude that its privacy focus is unmistakable.

3. Legislative History

We consult the Act's legislative history to test our conclusion.

In enacting the SCA, Congress expressed a concern that developments in technology could erode the privacy interest that Americans traditionally enjoyed in their records and communications. *See* S. Rep. No. 99-541, at 3 ("With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information."); H.R. Rep. No. 99-647, at 19 (1986) ("[M]ost important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."). In particular, Congress noted that the actions of private parties were largely unregulated when it came to maintaining the privacy of stored electronic communications. *See* S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 18. And Congress observed further that recent Supreme Court precedent

called into question the breadth of the protection to which electronic records and communications might be entitled under the Fourth Amendment. *See* S. Rep. No. 99-541, at 3 (citing *United States v. Miller*, 425 U.S. 435 (1976), for proposition that because records and private correspondence in computing context are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection"); H.R. Rep. No. 99-647, at 23 (citing *Miller* for proposition that "under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services").

Accordingly, Congress set out to erect a set of statutory protections for stored electronic communications. *See* S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 19. In regard to governmental access, Congress sought to ensure that the protections traditionally afforded by the Fourth Amendment extended to the electronic forum. *See* H.R. Rep. No. 99-647, at 19 ("Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment."). It therefore modeled § 2703 after its understanding of the scope of the Fourth Amendment. As the House Judiciary Committee explained in its report, it appeared likely to the Committee that "the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required." *Id.* at 22.

We believe this legislative history tends to confirm our view that the Act's privacy provisions were its impetus and focus. Although Congress did not overlook law enforcement needs in formulating the statute, neither were those needs the primary motivator for the enactment. *See* S. Rep. No. 99-541, at 3 (in drafting SCA, Senate Judiciary Committee sought "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs").

Taken as a whole, the legislative history tends to confirm our view that the focus of the SCA's warrant provisions is on protecting users' privacy interests in stored communications.

E. Extraterritoriality of the Warrant

Having thus determined that the Act focuses on user privacy, we have little trouble concluding that execution of the Warrant would constitute an unlawful extraterritorial application of the Act. *See Morrison*, 561 U.S. at 266–67; *RJR Nabisco*, 579 U.S. at __, 2016 WL 3369423, at *9.

The information sought in this case is the content of the electronic communications of a Microsoft customer. The content to be seized is stored in Dublin. J.A. at 38. The record is silent regarding the citizenship and location of the customer. Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government.[27] Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.[28] *Cf. Riley*

[27] We thus disagree with the magistrate judge that all of the relevant conduct occurred in the United States. *See In re Warrant*, 15 F. Supp. 3d at 475–76.

[28] The concurring opinion suggests that the privacy interest that is the focus of the statute may not be intrinsically related to the place where the private content is stored, and that an emphasis on place is "suspect when the content consists of emails stored in the 'cloud.'" Concurring Op. at 14 n.7. But even messages stored in the "cloud" have a discernible physical location. Here,

v. California, 134 S. Ct. 2473, 2491 (2014) (noting privacy concern triggered by possibility that search of arrestee's cell phone may inadvertently access data stored on the "cloud," thus extending "well beyond papers and effects in the physical proximity" of the arrestee).

The magistrate judge suggested that the proposed execution of the Warrant is not extraterritorial 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. . . . [I]t places obligations only on the service provider to act within the United States." *In re Warrant*, 15 F. Supp. 3d at 475–76. We disagree. First, his narrative affords inadequate weight to the facts that the data is stored in Dublin, that Microsoft will necessarily interact with the Dublin datacenter in order to retrieve the information for the government's benefit, and that the data lies within the jurisdiction of a foreign sovereign. Second, the magistrate judge's observations overlook the SCA's formal recognition of the special role of the service provider vis-à-vis the content that its customers entrust to it. In that respect, Microsoft is unlike the defendant in *Marc Rich* and other subpoena recipients who are asked to turn over records in which only *they* have a protectable privacy interest.

The government voices concerns that, as the magistrate judge found, preventing SCA warrants from reaching data stored abroad would place a "substantial" burden on the government and would "seriously impede[]" law enforcement efforts. *Id*. at 474.

---

we know that the relevant data is stored at a datacenter in Dublin, Ireland. In contrast, it is possible that the identity, citizenship, and location of the user of an online communication account could be unknown to the service provider, the government, and the official issuing the warrant, even when the government can show probable cause that a particular account contains evidence of a crime.

The magistrate judge noted the ease with which a wrongdoer can mislead a service provider that has overseas storage facilities into storing content outside the United States. He further noted that the current process for obtaining foreign-stored data is cumbersome. That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See* U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), *available at* fam.state.gov/FAM/07FAM/07FAM0960.html (last visited May 12, 2016) (discussing and listing MLATs).[29] And he observed that, for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad.[30]

These practical considerations cannot, however, overcome the powerful clues in the text of the statute, its other aspects, legislative history, and use of the term of art

---

[29] The United States has entered into an MLAT with all member states of the European Union, including Ireland. *See* Agreement on Mutual Legal Assistance Between the European Union and the United States of America, June 25, 2003, T.I.A.S. No. 10-201.1.

[30] In addition, with regard to the foreign sovereign's interest, the District Court described § 442 (1)(a) of the Restatement of Foreign Relations Law as "dispositive." Tr. of Oral Arg., *supra* note 25, at 69. That section provides:

> A court or agency in the United States, when authorized by statute or rule of court, [is empowered to] 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.

Restatement of Foreign Relations Law (3d) § 442(1)(a) (1987). We are not persuaded. The predicate for the Restatement's conclusion is that the court ordering production of materials located outside the United States is "authorized by statute or rule of court" to do so. Whether such a statute—the SCA—can fairly be read to authorize the production sought is precisely the question before us.

"warrant," all of which lead us to conclude that an SCA warrant may reach only data stored within United States boundaries. Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations. Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign—and in particular, here, of Ireland or the E.U.—place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States.

Thus, to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act.

CONCLUSION

We conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland. Because Microsoft has otherwise complied with the Warrant, it has no remaining lawful obligation to produce materials to the government.

We therefore **REVERSE** the District Court's denial of Microsoft's motion to quash; we **VACATE** its order holding Microsoft in civil contempt of court; and we **REMAND** this cause to the District Court with instructions to quash the warrant insofar as it demands user content stored outside of the United States.