No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

ON WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

BRIEF FOR RESPONDENT

Bradford L. Smith
David M. Howard
Julie Brill
John Frank
Jonathan Palmer
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

James M. Garland
Alexander A. Berengaut
Lauren K. Moxley
COVINGTON & BURLING LLP
850 10th Street NW
Washington, DC 20001

E. Joshua Rosenkranz
Counsel of Record
Robert M. Loeb
Brian P. Goldman
Evan M. Rose
Hannah Garden-Monheit
Alec Schierenbeck
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000
jrosenkranz@orrick.com

Counsel for Respondent

QUESTION PRESENTED

The Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, a part of the Electronic Communications Privacy Act of 1986, protects communications entrusted to email providers from threats like hacking, publication by providers, and unauthorized government searches and seizures. It contains a limited exception that allows federal, state, and local law-enforcement officers to require providers to turn over email content "only pursuant to a warrant." § 2703(a).

The Government invoked § 2703 to require Microsoft to assist it with executing a warrant to search and seize all the private correspondence in an individual's account on a Microsoft email service. That email content, however, is processed and stored on a Microsoft server in Dublin, Ireland, where it is regulated and protected by Irish and EU data-privacy laws and those sovereigns' own rules governing law-enforcement access. It is undisputed here that Congress did not expressly provide for extraterritorial application of the SCA, which means that the Act may not be applied abroad given the presumption against extraterritoriality.

The question presented is:

Whether invoking the SCA's law-enforcement exception to demand the importation of private electronic communications stored in a foreign country is an impermissible extraterritorial application of the Act.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

TABLE OF AUTHORITIES v

INTRODUCTION 1

STATUTORY PROVISIONS INVOLVED 4

STATEMENT OF THE CASE..... 4

SUMMARY OF ARGUMENT..... 11

ARGUMENT 14

I. Congress Gave No Indication That The Stored Communications Act Should Apply Extraterritorially. 14

II. A Warrant Requiring The Copying And Importation Of Communications Stored Overseas Is An Impermissible Extraterritorial Application Of The Stored Communications Act. 19

A. The SCA, including § 2703, covers only communications stored in the United States because its focus is protecting "communications in electronic storage," not "disclosure."..... 20

1. Section 2703 is part of an interlocking trio of substantive provisions focused on protecting "communications in electronic storage."..... 22

2. Even in isolation, § 2703 focuses on protecting "communications in electronic storage." 25

3. A focus on "disclosure" would have left gaps in coverage in 1986 that are inconsistent with Congress's clear intention. 29

B. The conduct that the SCA compels is a law-enforcement seizure, which occurs where the private correspondence is stored. 32

C. The international discord that has erupted, and the potential for conflict with foreign laws, confirm that the warrant entails an impermissible extraterritorial application of the SCA. 37

III. Pre-*Morrison* Cases Addressing A Subpoena's Global Reach Shed No Light On The Focus Of The SCA's Warrant Provision. 44

IV. The Government's Policy Concerns Are Properly Addressed To Congress. 51

CONCLUSION 62

APPENDIX

Relevant Statutory and Regulatory Provisions

18 U.S.C. § 1030(e)(2)(B) (current) 1a

18 U.S.C. § 2701(a), (c) (current) 1a

18 U.S.C. § 2702(a)-(c) (current) 2a

18 U.S.C. § 2703 (a)-(d), (g) (current) 6a

18 U.S.C. § 2703(a) (Oct. 26, 2001)..... 10a
18 U.S.C. § 2703(a) (1986) 11a
18 U.S.C. 2706(a) (current)..... 12a
18 U.S.C. § 2707(a)-(c) (current)..... 12a
18 U.S.C. § 2711(3)-(4) (current) 13a
18 U.S.C. § 2711(3) (Oct. 26, 2001)..... 14a
18 U.S.C. § 3127(2) (Oct. 26, 2001)..... 15a
18 U.S.C. § 3512(a), (d), (f) (current)..... 15a
Fed. R. Crim. P. 41 (current) 17a
Fed. R. Crim. P. 41(a) (1986) 26a
Commission Regulation 2016/679,
2016 O.J. (L 119) 64 (arts. 48 & 49) 26a

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Arizona v. United States,
567 U.S. 387 (2012).....16

BedRoc Ltd. v. United States,
541 U.S. 176 (2004).....25

Benz v. Compania Naviera Hidlago, S.A.,
353 U.S. 138 (1957).....52

California Bankers Ass'n v. Shultz,
416 U.S. 21 (1974).....33

Donovan v. Lone Star Steer, Inc.,
464 U.S. 408 (1984).....48

EEOC v. Arabian Am. Oil Co.,
499 U.S. 244 (1991).....10, 14, 27, 38, 54

F. Hoffman-La Roche Ltd. v. Empagran S.A.,
542 U.S. 155 (2004).....15, 16, 40, 53

*Fisher v. United State*s,
425 U.S. 391 (1976).....50

In re Horowitz,
482 F.2d 72 (2d Cir. 1973) 50

Katz v. United States,
389 U.S. 347 (1967).....35

Kiobel v. Royal Dutch Petroleum Co.,
569 U.S. 108 (2013).....14, 24

Kyllo v. United States,
533 U.S. 27 (2001).....36

Marc Rich & Co. v. United States,
707 F.2d 663 (2d Cir. 1983) 44

Mastafa v. Chevron Corp.,
770 F.3d 170 (2d Cir. 2014) 37

Microsoft Corp. v. AT&T Corp.,
550 U.S. 437 (2007).....2, 27, 39

Morrison v. Nat'l Austl. Bank Ltd.,
561 U.S. 247 (2010).....9, 14, 20, 25, 28, 30, 37, 50

Murray v. The Schooner Charming Betsy,
6 U.S. (2 Cranch) 64 (1804) 40

Oklahoma Press Pub. Co. v. Walling,
327 U.S. 186 (1946).....48, 51

Rakas v. Illinois,
439 U.S. 128 (1978).....36

Riley v. California,
134 S. Ct. 2473 (2014).....3, 36, 51

RJR Nabisco, Inc. v. European Cmty.,
136 S. Ct. 2090 (2016).....15, 18, 20, 25, 30, 39, 40

Skinner v. Ry. Labor Execs.' Ass'n,
489 U.S. 602 (1989).....33

Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522 (1987).....50

United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).....35

United States v. Bach, 310 F.3d 1063 (8th Cir. 2002).....35, 47

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).....35

United States v. First Nat'l City Bank, 396 F.2d 897 (2d Cir. 1968) 51

United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001) 36

United States v. Jacobsen, 466 U.S. 109 (1984).....34

United States v. Miller, 425 U.S. 435 (1976).....5, 23

United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297 (1972).....35

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).....15

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).....6, 34, 35, 49

Utility Air Regulatory Grp. v. EPA,
134 S. Ct. 2427 (2014).....25

Weinberger v. Rossi,
456 U.S. 25 (1982).....40

Constitutional Provisions

U.S. Const. amend. IV 4, 6, 22, 26, 36

Statutes, Rules & Regulations

18 U.S.C. § 1030(e)(2)(B) 18

Stored Communications Act (SCA),
18 U.S.C. § 2701 *et seq.*

18 U.S.C. § 2701.....5, 11, 12, 22, 23, 24

18 U.S.C. § 2701(a) 23

18 U.S.C. § 2701(c)(3) 5, 23

18 U.S.C. § 2702.....5, 11, 12, 23, 24, 29, 30, 31

18 U.S.C. § 2702(a)(1).....23

18 U.S.C. § 2702(b)(2).....5, 23, 29

18 U.S.C. § 2702(c).....45

18 U.S.C. § 2703.....*passim*

18 U.S.C. § 2703(a) .....i, 6, 8, 23, 45, 46, 47, 48

18 U.S.C. § 2703(b) 48, 64

18 U.S.C. § 2703(c).....45, 48

18 U.S.C. § 2703(c)(2) 6, 45

18 U.S.C. § 2703(d) 6, 29, 48

18 U.S.C. § 2703(e) 23

18 U.S.C. § 2703(g) 6, 12, 27, 29, 32, 47

18 U.S.C. § 2706.....6

18 U.S.C. § 2706(a) 33

18 U.S.C. § 2707.....23, 31

18 U.S.C. § 2711(4) 5, 15, 26, 27

18 U.S.C. § 3105.....6

18 U.S.C. § 3486.....46

Civil Rights Act of 1991, Pub. L. No. 102-166, 105 Stat. 1071 54

Foreign Evidence Request Efficiency Act of 2009, Pub. L. No. 111-79, 123 Stat. 2086.....18

USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).....17

Fed. R. Civ. P. 34(a)(1).....46

Fed. R. Civ. P. 45(a)(1)(A)(iii) 46

Fed. R. Crim. P. 16(a)(1).....46

Fed. R. Crim. P. 16(b)(1) 46

Fed. R. Crim. P. 17(c) 46

Fed. R. Crim. P. 41 .....17, 47

Fed. R. Crim. P. 41(a) (1986) 17

Fed. R. Crim. P. 41(e)(2)(B) 35

Legislative Authority

147 Cong. Rec. H7197-98
(daily ed. Oct. 23, 2001) 17

155 Cong. Rec. S6809
(daily ed. June 18, 2009).....18

H.R. Rep. No. 99-647 (1986) 4, 5, 37, 46, 49, 61

H.R. Rep. No. 107-236 (2001) 17

H.R. Rep. No. 107-497 (2002) 47

H.R. Rep. No. 114-528 (2016) 6

S. Rep. No. 99-541 (1986).....4, 5, 6, 16, 21, 23, 46

Other Authorities

Brief for United States, *Carpenter v. United States*, No. 16-402 (U.S. Sept. 25, 2017) 46

Commission Regulation 2016/679, 2016 O.J.
(L 119) 64 41

George B. Delta & Jeffrey H. Matsuura, *Law of the Internet* (4th ed. 2018) 16

Einer Elhauge, *Statutory Default Rules: How to Interpret Unclear Legislation* (2008).....54

Hearing Transcript, *In re Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-80263 (N.D. Cal. Aug. 10, 2017) 60

International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Judiciary Comm. (Feb. 25, 2016), https://perma.cc/Z2ZE-PQ8F (testimony of Brad Smith, President and Chief Legal Officer, Microsoft Corp.) 58

International Communications Privacy Act, S. 1671, 115th Cong. (2017).....52, 53

Ireland Data Protection Commissioner, *Transfers Abroad*, https://perma.cc/96V2-MHNW 42

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 (2004) 6

Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373 (2014).....16, 17

Law Enforcement Access to Data Stored Across Borders: Hearing Before the S. Subcomm. on Crime and Terrorism (May 24, 2017), https://perma.cc/6GME-GXCH (testimony of Brad Wiegmann, Deputy Assistant Att'y Gen., U.S. Dep't of Justice) 40

Letter from Samuel R. Ramer, Acting Assistant Att'y Gen., U.S. Dep't of Justice, to Hon. Paul Ryan, Speaker, U.S. House of Reps., (May 24, 2017), https://perma.cc/MUT6-A8GC 52

Microsoft, *Delivering a Faster and More Responsive Outlook.com* (Oct. 27, 2017), https://perma.cc/MZ8Y-JT7P 57

Office of Tech. Assessment, U.S. Cong., Fed. Gov't Info. Tech., *Electronic Surveillance and Civil Liberties* (1985), https://perma.cc/52RK-ALLF 16

ProtonMail, *Security*, https://perma.cc/C2MF-5HZQ 56

Restatement (Third) of the Foreign Relations Law of the United States (2017).....39, 51

Statement of the Art. 29 Working Party (Nov. 29, 2017), https://perma.cc/5EM2-7F9K 42

Transcript of Oral Argument, *Carpenter v. United States*, No. 16-402 (U.S. Nov. 29, 2017) 46, 52

U.S. Dep't of Justice, *U.S. Attorneys' Manual, Criminal Resource Manual*, https://perma.cc/3SYM-7VJ7 41

INTRODUCTION

The Government concedes that Congress never clearly indicated that the Stored Communications Act should reach private communications stored on computers in foreign countries. No surprise for a statute enacted in 1986, before the global internet, when Congress could scarcely have imagined the possibility of remotely accessing emails stored halfway across the world. Back then, if the Government wanted to seize a trove of private letters stored in a foreign country, it would have had to request the foreign government's assistance. There is no indication Congress thought electronic letters would be any different. And in enacting a statute to *restrict* law-enforcement access to personal communications, Congress never suggested that it was globally *expanding* the Government's power to seize them.

The Government raises policy arguments for extending the statute to private email stored in foreign countries. This is not the forum for that debate. Congress is currently weighing proposals—including one submitted by the Government—to modify the SCA's reach to account for the dramatic leaps in technology over the last three decades. There are many reasons Congress might stop short of granting the full power the Government seeks: It would instigate a global free-for-all, inviting foreign governments to reciprocate by unilaterally seizing U.S. citizens' private correspondence from computers in the United States. It would offend foreign sovereigns. And—especially given foreign governments' and businesses' sensitivities in the wake of recent revelations about the U.S.

Government's surveillance practices—it would jeopardize U.S. technology companies' position atop the $250 billion cloud-computing industry.

The Government counters with the benefits of allowing law enforcement to reach everyone's communications, everywhere. Congress might balance those competing interests by expanding the SCA to reach only U.S. citizens' and residents' communications stored abroad. It might grant the extraordinary power the Government claims here, but only to the federal government—not to state and local officials, who the current statute treats equivalently. Or it might not expand the SCA at all.

This Court should not preemptively perform the delicate surgery that this aged statute needs with the blunt tool urged by the Government: reading the current text to apply to *all* emails stored in other countries. Only Congress can "create nuanced rules" that avoid this "all-or-nothing choice." Pet. App. 69a (Lynch, J., concurring). Any updates must "be made after focused legislative consideration, and not by the Judiciary forecasting Congress' likely disposition." *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 459 (2007).

Meanwhile, the presumption against extraterritoriality makes this Court's job simple: Because statutes apply only domestically unless Congress clearly indicates otherwise, the SCA should be read to apply only to electronic communications stored here, just as other countries' laws govern electronic communications stored on their soil. This rule ensures that courts do not trigger international discord—like the outcry that the Government's order to Microsoft has

prompted from foreign leaders around the world. That response was to be expected. If a foreign government unilaterally seized an American's most personal documents stored in the United States—whether in a home, safe-deposit box, or computer server—the U.S. Government and the American public would react the same way.

The Government's contrary argument reads the statute, which Congress enacted to *protect* the security of "communications in electronic storage," to focus instead on *facilitating* the "disclosure" of communications. It defends its reading with lower-court decisions allowing subpoenas to order a company to gather its own business records, regardless of their location. But that argument recasts "warrants" as "subpoenas," treats the private "contents of electronic communications" owned by customers as a company's own business "records," and equates ordering a provider to "execut[e] a search warrant" with the act of "gather[ing] … responsive materials." For an argument that purports to rest on the statute's plain text, the Government rewrites an awful lot of it.

Just as this Court declined, in *Riley v. California*, 134 S. Ct. 2473 (2014), to expand the search-incident-to-arrest exception from the contents of cigarette packs to the contents of smartphones, it should refuse to stretch rules governing business records held abroad to the "qualitative[ly]" and "quantitative[ly]" distinct cache of intimate letters, diaries, and photos that people around the world now entrust to third-party providers for secure electronic storage. *Id.* at 2488-89.

The judgment should be affirmed.

STATUTORY PROVISIONS INVOLVED

Relevant statutory provisions are reproduced in the appendix to this brief.

STATEMENT OF THE CASE

A. In the 1980s, Congress understood that a wave of emerging communications technologies, including "[e]lectronic mail," might replace paper letters. H.R. Rep. No. 99-647, at 21-23 (1986). But it worried that technological advancement would be stunted if electronic communications lacked the protections afforded to the contents of sealed envelopes. S. Rep. No. 99-541, at 3-5 (1986).

These new technologies required account owners to entrust their sensitive communications to private companies—"new noncommon carrier … services" using "new forms of … computer technology." *Id.* at 5. And "even though American citizens and American businesses [were] using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services," "legal uncertainty" abounded. *Id.* Whereas the Wiretap Act protected spoken communications from interception during transmission, "there [were] no comparable Federal statutory standards to protect the privacy and security of communications" in writing that were now transmitted—and could be indefinitely stored—using this new, private delivery system. *Id.*

Congress also feared courts might strip digital letters of the Fourth Amendment protection accorded to paper letters—on the ground that users relinquish

privacy protections under the "third-party doctrine" when they voluntarily share their email with service providers. *Id.* at 3; H.R. Rep. No. 99-647, at 23 & nn.40-41, 72-73 (all discussing *United States v. Miller*, 425 U.S. 435 (1976)). It worried that increased use of "computers … for the storage and processing of information" could thus lead to a "gradual erosion" of the "precious right" to privacy. S. Rep. No. 99-541, at 3, 5.

In 1986, Congress addressed these concerns by enacting the Electronic Communications Privacy Act (ECPA). Title II of ECPA is known as the Stored Communications Act. It protects communications sent electronically and stored by a service provider, treating them like communications sent by post and stored in locked drawers. The SCA protects "communications … in electronic storage" from unauthorized access by hackers and rogue employees (§ 2701), voluntary disclosure by providers (§ 2702), and unwarranted search and seizure by law enforcement (§ 2703). These provisions are interconnected and inseparable. Section 2703, for example, carves out a limited exception to the categorical bans of §§ 2701 and 2702. *See* § 2701(c)(3); § 2702(b)(2).

Section 2703 prevents law-enforcement officers—federal, state, and local, *see* § 2711(4)—from obtaining stored private communications and related information from providers without proper process. It protects against application of the third-party doctrine to the contents of private communications in electronic storage, by allowing law enforcement to obtain them "only pursuant to a warrant" using federal or state

warrant procedures.[1] And § 2703(g) creates an express exception to the ordinary requirement that an officer execute the warrant herself, *see* § 3105. Instead, law enforcement may outsource "execution of [the] search warrant," § 2703(g), by compelling providers to "search[] for, assembl[e], [and] reproduce[]" the targeted documents at law enforcement's expense, § 2706.

Other subsections of § 2703 treat *non-content* information—like the customer's name or the addressee of an electronic message—differently. As with a mailed letter, law enforcement can obtain this "envelope" information without a warrant—sometimes by subpoena, § 2703(c)(2), and sometimes by a novel form of order issued under § 2703(d).

---

[1] Section 2703(a) requires a warrant only for emails up to 180 days old, because in 1986 those were the only ones considered to be private: Emails were ordinarily retrieved promptly by the customer and then deleted from the provider's computer. Thus, copies of emails left with the provider for over six months were considered to have no more protection than abandoned scraps of paper. *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, 1234 (2004); H.R. Rep. No. 99-647, at 68; *see* S. Rep. No. 99-541, at 3, 8. Now, of course, customers use email services very differently, leading courts to hold that the Fourth Amendment requires a warrant to obtain all email content, regardless of age. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). Accordingly, "the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013." H.R. Rep. No. 114-528, at 9 (2016).

B. Microsoft operates a web-based email service called Outlook.com. J.A. 30. It allows customers to remotely access and manage their messages from anywhere just by connecting to the internet. Colloquially, we say that emails are stored in the "cloud." But the storage is every bit as terrestrial as a post-office box. A customer's private correspondence is stored on the physical hard drive of a computer server housed in a datacenter. J.A. 30, 42.

Microsoft operates datacenters located around the world. It strives to store emails close to their owner to boost the quality of service. J.A. 31. Proximity reduces "network latency," which is the phenomenon of service slowing as data has to travel further through physical cable. *Id.* Thus, Microsoft assigns accounts to the appropriate datacenter almost immediately after creation. J.A. 31. One of Microsoft's datacenters is a 584,000-square-foot, state-of-the-art facility in Dublin, Ireland. When Microsoft assigns a customer's account to the Dublin datacenter, it does not store copies of the account within the United States. J.A. 30-32.

Microsoft receives tens of thousands of demands for electronic communications each year from federal, state, and local governments, as well as foreign governments. When Microsoft receives a lawful order from U.S. authorities, a Microsoft employee determines the location of the datacenter where the targeted emails are stored. For correspondence stored in the United States, the employee copies the emails from the domestic server and transmits them to U.S. law enforcement as the warrant commands. Pet. App. 76a-77a. But when a law-enforcement officer

seeks emails stored in Dublin, Microsoft has directed officers to the United States-Ireland Mutual Legal Assistance Treaty (MLAT), which allows the U.S. Government to obtain emails with the cooperation of the Irish Ministry of Justice. J.A. 47-49.

C. In 2013, federal agents conducting a drug investigation obtained a warrant to search and seize "all e-mails" stored in a customer's webmail account and "all … other information" related to the account. J.A. 22-26. The Government faxed the warrant to Microsoft and directed it to send the target customer's communications to federal agents. Pet. App. 2a. The Government has never suggested that the customer is a citizen or resident of the United States. Pet. App. 21a.

Microsoft turned over all the account information that was stored in the United States, including the contents of the customer's electronic "address book." J.A. 32, 34-35. But Microsoft determined that the emails targeted by the warrant were stored in Dublin. J.A. 34. Microsoft therefore moved the magistrate judge to vacate the warrant insofar as it ordered Microsoft to seize communications stored in a foreign country.

The magistrate judge denied the motion. He recognized that § 2703(a)'s plain text uses the term "warrant." Pet. App. 84a. But he held that word was better read to mean a "hybrid: part search warrant and part subpoena." *Id.* Invoking cases involving subpoenas for a company's own business records, he ordered Microsoft to turn over the customer's private correspondence stored in Ireland. Pet. App. 97a.

The District Court summarily affirmed, Pet. App. 100a-102a, and held Microsoft in contempt for refusing to comply with the Warrant. Pet. App. 103a.

D. A unanimous panel of the Second Circuit reversed. Applying the two-step extraterritoriality framework from *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), the court concluded that "the District Court lacked authority to enforce the Warrant against Microsoft" because "[n]either explicitly nor implicitly does the statute envision the application of its warrant provisions overseas." Pet. App. 4a-5a, 22a. At the first step, the court held that the SCA has no extraterritorial application. It noted that the Government had "conceded" that "the warrant provisions of the SCA do not contemplate or permit extraterritorial application." Pet. App. 23a-24a. The court confirmed that, in enacting the SCA, Congress did not provide for extraterritorial reach: Congress used the territorial term "warrant," apart from the term "subpoena"; and there is no indication that the Congress of 1986 would have envisioned "a globally-connected Internet available to the … public for routine e-mail" use. Pet. App. 14a, 23a.

Proceeding to *Morrison*'s second step, the court concluded that the Government was seeking to apply the SCA extraterritorially by requiring that email be "seized" from storage in Dublin. Pet. App. 44a-47a. The court explained: "[T]he relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored … communications." Pet. App. 37a. Thus, the location where the SCA is applied is where

the communications are stored, not where the provider would ultimately turn them over to the Government. Pet. App. 43a-47a.

The Court of Appeals found corporate subpoena cases inapposite: The Government did not seek Microsoft's own records, but rather private emails of which Microsoft is a mere "caretaker." Pet. App. 34a-35a, 44a-45a. The court also reasoned that its interpretation of the SCA would avoid "conflicts with foreign laws and procedures" that Congress did not authorize—particularly given that § 2703 equally empowers state and local law-enforcement officers to use its full reach. Pet. App. 25a (quoting *EEOC v. Arabian Am. Oil Co.* (*Aramco*), 499 U.S. 244, 256 (1991)); *see* Pet. App. 44a-46a.

Judge Lynch concurred. "Despite [his] hesitation" about the outcome, he concluded that "[i]f we frame the question as whether Congress has demonstrated a clear intention to reach situations of this kind …, I think the better answer is that it has not, especially in the case (which could well be this one) of records stored at the behest of a foreign national on servers in his own country." Pet. App. 66a-67a. Indeed, there was no indication Congress "had given any thought at all to potential transnational applications of the statute." Pet. App. 67a-68a. Because Congress had never "weighed the costs and benefits of authorizing court orders of the sort at issue in this case," Judge Lynch "emphasize[d] the need for congressional action to revise a badly outdated statute." Pet. App. 49a, 68a. He called on "the Justice Department [to] respond to this decision by seeking legislation" to "create nuanced

rules" that only Congress, not the courts, can provide. Pet. App. 69a, 71a.

The Court of Appeals denied the Government's rehearing petition by a 4-4 vote, with three judges recused. Judge Carney concurred in the denial of rehearing. Pet. App. 107a-119a. Four judges dissented from the denial. Pet. App. 120a-154a.

SUMMARY OF ARGUMENT

I. Congress never envisioned, let alone clearly indicated, that the SCA should apply to communications stored overseas. Under the presumption against extraterritoriality, the statute therefore does not apply abroad.

II. The Government insists that it is invoking the SCA only domestically when it demands that Microsoft retrieve emails from a physical computer in Ireland, copy them, and import them into the United States, because the ultimate disclosure of the emails would occur here. But the most straightforward reading of the SCA is that it protects domestically stored communications (wherever disclosed), not domestically disclosed communications (wherever stored).

A. The SCA's focus—the object of Congress's solicitude—is not "disclosure"; it is protecting the security of "electronic communication[s]" that customers entrust to third-party providers for safekeeping "in electronic storage." It is those "communications in electronic storage" that Congress sought to protect from hackers or rogue employees (§ 2701), unreliable providers (§ 2702), and government agents (§ 2703).

So the SCA is applied where the communications are stored.

The Government does not suggest that §§ 2701 and 2702 protect "communications in electronic storage" overseas. It argues, however, that § 2703—a limited law-enforcement exception to those provisions—should be read in isolation. But isolating § 2703 from the provisions that cross-reference it is inconsistent with basic principles of statutory interpretation.

Even taking § 2703 in isolation, however, its focus is also "communications in electronic storage." Congress adopted § 2703 to protect those communications *against* governmental intrusions—not to facilitate broad access. Moreover, the Government's disclosure-focused construction would create strange gaps in coverage Congress plainly did not intend: It would leave U.S. citizens' U.S.-stored communications unprotected, so long as they were disclosed overseas.

B. The conduct that § 2703 commands is the "execution of a search warrant," § 2703(g)—and that would occur overseas. The place to be searched and the things to be seized are emails located on a physical computer server in a datacenter in Dublin, where Irish and EU law protects them. Those emails would be seized in Ireland, where Microsoft would be compelled to copy and transmit them to the United States on the Government's behalf. That the Government has outsourced this activity to a service provider does not change the location of the law-enforcement operation or mitigate the incursion on foreign sovereignty. It is a Government-initiated intrusion upon the account owner's property rights all the same. Nor does

it matter that the seizure is effected remotely. A remote seizure occurs where the seized object is located, not where the operator happens to sit.

C. The international outcry this warrant has sparked confirms that it involves just the sort of projection of U.S. law abroad that the presumption against extraterritoriality is meant to avoid. Leaders across Europe have lambasted the Government's attempt to "circumvent[] … existing MLATs … [and] interfere[] with the territorial sovereignty of an EU member state." The Government's reading of the SCA will also produce direct conflicts with foreign laws that govern emails stored in foreign lands. Until and unless Congress exercises its sole prerogative to assume the risk of such international discord, the SCA reaches only emails stored here.

III. The Government attempts to shoehorn this case into lower-court cases allowing subpoenas to reach a company's own business records that are located overseas. But the statute says "warrant," not "subpoena," and it expressly distinguishes email "content" from mere business "records." So the cases the Government invokes do not apply, and there is no reason to think Congress expected they would. Besides, no court has ever held that subpoenas may reach private correspondence stored with a custodian in a foreign country. The doctrine allowing subpoenas to reach abroad is fraught enough when applied to business records; it should not be *extended* to vast amounts of personal data stored overseas.

IV. The Government rests heavily on policy concerns arising from the ill fit between the SCA and today's globally connected world. But only Congress has the authority and tools to rewrite the statute to strike a new, 21st-century balance between law-enforcement interests, our relations with foreign nations, the privacy of our citizens, and the competitiveness of our technology industry. The current Congress has been considering multiple proposals to do just that—including one urged by the Government itself. Until Congress acts, the SCA applies only to emails stored here. In the meantime, the Government may rely on the international cooperative mechanisms it has used for decades to obtain evidence located in foreign countries.

ARGUMENT

I. Congress Gave No Indication That The Stored Communications Act Should Apply Extraterritorially.

A. This Court has repeatedly emphasized that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 248. This "presumption against extraterritoriality" guards against projecting U.S. authority abroad absent the express blessing of the political branches. *See Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 115-17 (2013). It ensures that courts do not apply statutes in ways that risk "unintended clashes between our laws and those of other nations." *Aramco*, 499 U.S. at 248. And it prevents courts from accidentally disrupting the "harmony" between nations

that is "particularly needed in today's highly interdependent commercial world." *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164-65 (2004).

Applying the presumption begins with asking whether Congress gave "a clear, affirmative indication that [a statute] applies extraterritorially." *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016). Nothing in the SCA "even implicitly alludes to any … application" to emails stored overseas. Pet. App. 24a. The SCA is not just silent, though. Two aspects of its text confirm that Congress intended it to reach only communications located within the United States.

First, Congress required law enforcement to secure a "warrant" to obtain private electronic communications. "Warrant" is a legal term of art that carries a territorial limitation: A "warrant" is a "dead letter outside the United States." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990). "[I]t is hard to believe that Congress would have used such a loaded term, and incorporated by reference the procedures applicable to purely domestic warrants, if it had given any thought at all to potential transnational applications of the statute." Pet. App. 67a (Lynch, J., concurring).

Second, the SCA authorizes "any State or political subdivision thereof," § 2711(4), to obtain emails from a provider with a warrant, not just the federal government. It is "particularly unlikely" that Congress would have entrusted to local sheriffs and police departments the power to seize evidence from foreign countries. Pet. App. 25a. Like any nonfederal actors,

state and local officials typically are ill-equipped to "exercise the degree of self-restraint and consideration of foreign governmental sensibilities generally exercised by the U.S. Government." *Empagran*, 542 U.S. at 171 (citation omitted). Because they have no authority to conduct foreign relations, *e.g.*, *Arizona v. United States*, 567 U.S. 387, 409 (2012), they are unable to make the nuanced diplomatic tradeoffs such foreign seizures require.

B. The SCA's historical context and subsequent amendments further confirm that Congress never extended it to emails located overseas. When it enacted the SCA over "thirty years ago, Congress had as reference a technological context very different from today's Internet-saturated reality." Pet. App. 14a. "The *World Wide* Web was not created until 1990, and we did not even begin calling it that until 1993." *Id.* (emphasis added). In 1986, the services that brought email to the general public were still years away. *See generally* George B. Delta & Jeffrey H. Matsuura, *Law of the Internet* § 1.02 (4th ed. 2018). Back then, a service provider would often print an electronic message "and then deposit it in the normal postal system." S. Rep. No. 99-541, at 8. It was not until 1989 that America Online first played the "You've got mail!" message. Microsoft's Hotmail, the first major web-based email service, did not launch until 1996. And because phone lines transmitted electronic communications, international calling rates made international electronic messaging prohibitively expensive and effectively unavailable. *See* Office of Tech. Assessment, U.S. Cong., Fed. Gov't Info. Tech., *Electronic Surveillance and Civil Liberties* 46 (1985), https://perma.cc/52RK-ALLF; Orin S. Kerr, *The Next*

Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 404 & n.176 (2014). In short, Congress was "focused on the rights of U.S. computer users and U.S. services." Kerr, *supra*, at 405.

Subsequent amendments to the SCA only reinforced its territorial limits. As enacted, the SCA required federal warrants to be issued under Federal Rule of Criminal Procedure 41, which authorized warrants to issue only "within the district wherein the property … sought is located." Fed. R. Crim. P. 41(a) (1986). In 2001, to reduce "investigative delays," H.R. Rep. No. 107-236, at 57 (2001), Congress erased borders with respect to searches *within* the United States. It crafted an exception to Rule 41's within-district provision to allow "*Nationwide* Service of Search Warrants for Electronic Evidence," USA PATRIOT Act, Pub. L. No. 107-56, § 220, 115 Stat. 272, 291 (2001) (emphasis added), allowing "a single court having jurisdiction over the offense to issue a search warrant for e-mail that would be valid … anywhere *in the United States*." 147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) (emphasis added); H.R. Rep. No. 107-236, at 57. Congress did not say anywhere *in the world*. If Congress believed in 2001 that warrants issued under § 2703 already reached overseas—or thought that they now *should*—this would have been the place to mention it.

Indeed, in that very same legislation, Congress *expressly extended* a related 1986 statute, the Computer Fraud and Abuse Act, to protect "computer[s] located *outside the United States*" from certain acts of cybercrime. PATRIOT Act § 814(d)(1), 115 Stat. 384

(emphasis added); *see* 18 U.S.C. § 1030(e)(2)(B). Yet it left the SCA limited to the United States.

In 2009, Congress again revised the SCA. The Foreign Evidence Request Efficiency Act aimed to speed the Government's response when foreign governments request electronic evidence—including emails—stored here. Pub. L. No. 111-79, § 2, 123 Stat. 2086. Congress explained that "increasingly global" crime requires governments to "assist[] [one] another … by gathering evidence from *within [their] borders*." 155 Cong. Rec. S6809 (daily ed. June 18, 2009) (emphasis added). "[S]etting a high standard [for] [U.S.] responsiveness will allow the United States to urge that foreign authorities respond to our requests for evidence with comparable speed." *Id.* at S6810. The Act accordingly served to "greatly facilitate the ability of the U.S. government to meet its obligations under" "[MLATs] and multilateral conventions." *Id.* Thus, Congress reiterated its understanding that U.S. warrants reach only evidence "within [our] borders." *Id.* at S6809. It also confirmed that bilateral cooperation is the normal route for law enforcement in one country to access emails stored in another.

The Court of Appeals therefore correctly held—and the Government does not contest—that the SCA gives no "clear, affirmative indication that it applies extraterritorially." *RJR Nabisco*, 136 S. Ct. at 2101.

II. A Warrant Requiring The Copying And Importation Of Communications Stored Overseas Is An Impermissible Extraterritorial Application Of The Stored Communications Act.

The Government's position is paradoxical. It concedes (Br. 17) that Congress must be understood to have intended the SCA to apply only within U.S. borders. Yet it reads the SCA to reach emails stored outside U.S. borders. The Government does not dispute that the electronic correspondence in question has a physical location—on a hard drive in a physical facility in Dublin—where it is governed by Irish and EU law. Nor does it dispute that, when it compels Microsoft to help execute an SCA warrant, Microsoft must instruct a physical computer in Ireland to search for and copy the correspondence on its physical hard drive and then import that copy into the United States. *See* Computer Scientists Br. § II. Nevertheless, the Government insists that this is a merely "domestic" act. To the Government, all that matters is the ultimate act of "disclosure," which occurs here. The Second Circuit properly rejected the Government's effort to use *Morrison*'s second step to smuggle in a broad extraterritorial expansion of the SCA.

As the Court of Appeals held, what Congress sought to regulate and protect in enacting the SCA was the security of communications *in electronic storage*. Thus, at *Morrison* step two, this Court should read the statute to apply to domestically stored communications (wherever disclosed), not domestic disclosures of communications (wherever stored).

A. The SCA, including § 2703, covers only communications stored in the United States because its focus is protecting "communications in electronic storage," not "disclosure."

Morrison's second step recognizes that a statute's application sometimes entails a chain of activities, some local, some foreign. To "determine whether the case involves a domestic application of the statute," the Court "look[s] to the statute's 'focus.'" *RJR Nabisco*, 136 S. Ct. at 2101. "Focus" means "the objects of the statute's solicitude"—i.e., what Congress sought "to regulate" and "protect." *Morrison*, 561 U.S. at 266-67 (internal punctuation omitted). "[I]f the conduct relevant to th[at] focus occur[s] in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occur[s] in U.S. territory." *RJR Nabisco*, 136 S. Ct. at 2101.

Morrison applied the "focus" test to the Securities Exchange Act. It held that "the objects of the statute's solicitude" are "purchase-and-sale transactions" of securities. 561 U.S. at 267. Whether the Act could be applied to a particular securities-fraud claim therefore depends on the location of the *sale*, not the location where "the deception originated." *Id.* at 266-69. So the plaintiffs could not sue over a security traded outside the United States. *Id.* at 266, 273.

Applying that framework here presents this Court with a stark choice for identifying Congress's focus: secure storage of emails versus disclosure of emails. The Court of Appeals correctly held that the

focus of the *Stored Communications* Act is "protections for communications that are in electronic storage." Pet. App. 39a.[2] Congress's goal was to protect stored communications from hackers, unauthorized leakers, and unrestricted law-enforcement access. S. Rep. No. 99-541, at 5. The SCA thus governs only communications stored in the United States, Pet. App. 43a-44a, just as foreign law protects communications stored abroad.

The Government's proposed focus (Br. 17) is "disclosure." That would mean Congress intended the SCA to govern only communications ultimately *disclosed* in the United States; disclosures occurring outside the United States would be extraterritorial applications that the SCA does not reach. Under that reading, the SCA would provide no protection to the billions of emails U.S. citizens store in the United States, as long as the provider disclosed them outside the United States. This is highly improbable, given that Congress's priority was "to protect the privacy of our citizens," whose electronic communications were (and still generally are) stored in the United States. S. Rep. No. 99-541, at 5. But what matters most are the SCA's text, history, and context.

---

[2] The Court of Appeals did not hold that the SCA's focus is the "abstract concept" of "privacy," as the Government asserts throughout its brief. *E.g.*, Br. 26 (quoting Pet. App. 65a n.7). Rather, it held that the objects of the SCA's solicitude are the private *communications in electronic storage* that the statute protects. Pet. App. 38a-39a.

1. Section 2703 is part of an interlocking trio of substantive provisions focused on protecting "communications in electronic storage."

a. The SCA's text confirms that Congress enacted the SCA out of concern over the security of digital communications entrusted to third-party providers for remote storage. Specifically, Congress worried they could be more vulnerable to breaches of security—whether by hackers, providers themselves, or government agents—than paper letters transmitted by common carrier in sealed envelopes. Congress concluded digital "communications in electronic storage" deserved the same protections as letters sent by mail. *Supra* at 4-6. Just as the Fourth Amendment limits law-enforcement access to the content of letters in sealed envelopes or safe-deposit boxes, the SCA's law-enforcement provision protects the contents of electronic communications stored with email providers.

To accomplish this goal, Congress enacted the SCA's "three … major substantive provisions," Pet. App. 38a, which fit together like jigsaw pieces to protect the security of personal communications "in electronic storage":

> ***Section 2701*** "shelters the communications' integrity," Pet. App. 39a, by barring a form of hacking: "access[ing] without authorization a facility through which an electronic communication service is provided," to "obtain[]" an "electronic communication … in electronic storage."

Section 2702 addresses providers themselves, broadly prohibiting them from "divulg[ing] … the contents of a communication while in electronic storage," and subjecting them to civil liability for violating a customer's trust, § 2707.

Section 2703 limits the application of the third-party doctrine by restricting how law-enforcement officers may obtain private communications: "only pursuant to a warrant."

Section 2703 thus does not stand alone. It enables law enforcement to obtain otherwise-private communications "only as an exception to [the] primary obligations" of §§ 2701 and 2702. Pet. App. 39a; *see* §§ 2701(c)(3), 2702(b)(2), 2703(e). Congress adopted § 2703 as a limited "exception[]" "to the general rule of *non*disclosure." S. Rep. No. 99-541, at 37 (emphasis added). Its core purpose was to *limit* governmental access to digital letters to prevent "erosion of this precious right" to privacy, in the face of the third-party doctrine, *Id.* at 5; *see also id.* at 3 (citing *Miller*, 425 U.S. 435)—not "to protec[t] the government's interest in obtaining [them]." Gov't Br. 23 (quotation marks omitted).

Protecting the security of "communications … in electronic storage" with third-party providers is the common link that binds the three provisions together. These "parallel protections," Pet. App. 39a, each repeat the reference to the same location: communications "in electronic storage." §§ 2701(a), 2702(a)(1), 2703(a). They thus are applied where the communications are stored. This is true whether the party invoking the statute is the Government prosecuting a

hacker or rogue employee for unauthorized access under § 2701; a customer suing a provider for divulging his private communications under § 2702; or the Government seeking to seize a customer's private communications under § 2703.

In contrast, the focus the Government presses—"disclosure"—does not map onto the SCA's interlocking substantive provisions. Section 2701 does not address "disclosure" at all; it protects communications in electronic storage from hacking. And while § 2702 does mention "disclosure," Congress surely did not intend it to protect communications stored abroad from disclosure here. That would mean a foreign service provider could be haled into a U.S. court for divulging a foreign citizen's foreign-stored emails, just because those emails were disclosed here. *Cf. Kiobel*, 569 U.S. 118-24. Correspondingly, § 2703's law-enforcement exception must apply only to domestically stored communications. The provisions' shared language—"communication … in electronic storage"—cannot have a broader meaning in the exception (§ 2703) than in the core protections (§§ 2701 and 2702).

b. The Government does not contest that the focus of §§ 2701 and 2702 is the security of the stored communications themselves. It stakes the entire case on the proposition (Br. 18-21) that § 2703 has a different focus. But it offers no reason why Congress would craft a substantive rule that protects one universe of communications (those stored in the United States) with a limited law-enforcement exception that applies to a *broader* set (all emails, wherever stored, that can be accessed from within the United States).

The Government simply declares (Br. 18) that "the analysis must proceed on a provision-by-provision basis," such that the scope of one provision is irrelevant to the scope of its cross-referenced neighbors. That is not how this Court conducts statutory interpretation. Even where there is not such a close logical connection, the usual rule is that provisions that cross-reference each other are read together. *See, e.g.*, *Utility Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2441 (2014); *BedRoc Ltd. v. United States*, 541 U.S. 176, 185 (2004).

The Government incorrectly suggests (Br. 18-20) that *Morrison* and *RJR Nabisco* override this basic precept of statutory construction. To the contrary, *Morrison* itself identified the focus of § 10(b) of the Exchange Act in the context of related provisions of the Act, its prologue, and a separate statute enacted by the same Congress. *See* 561 U.S. at 266-69. *RJR Nabisco*, meanwhile, never even reached step two of the extraterritoriality analysis. *See* 136 S. Ct. at 2103-04; *see also id.* at 2111. It certainly did not hold—"implicitly" or otherwise, Gov't Br. 18-19—that the focus of every provision must be assessed in hermetic isolation.

2. Even in isolation, § 2703 focuses on protecting "communications in electronic storage."

a. Even accepting the Government's provision-by-provision approach, it is revisionist history to insist (Br. 23) that Congress enacted § 2703 to "protec[t] the government's interest in obtaining" stored communications. Even before the SCA, there was no doubt the

Government could obtain stored communications by warrant. What worried lawmakers was that courts would read the third-party doctrine to mean the Government could obtain them *without* a warrant. Congress thus enacted § 2703 largely because it wanted to *limit* the Government's access to stored communications. *Supra* at supra at4-6. The Government's argument is like saying that the Framers adopted the Fourth Amendment to protect the government's interest in obtaining evidence. Here, the Government complied with the warrant requirement. But the point is that the object of § 2703's solicitude—what the warrant protects against—is improper governmental intrusion on communications in storage, not insufficient disclosure to law enforcement.

Additional textual evidence confirms that Congress intended § 2703 to focus on the stored communications (in the United States) rather than domestic disclosure of communications (stored anywhere in the world):

First, consider which "governmental entities" can—and which cannot—invoke § 2703. State and local officers *are* included in the definition. § 2711(4). Those officers can—and regularly do—obtain orders under § 2703. That seems natural if Congress intended to focus on storage—and therefore to cover only emails stored in the United States. Problems abound, however, if § 2703 is read to authorize a sheriff's deputy in, say, Dublin, Florida, to instigate an international crisis by directing a search and seizure in Dublin, Ireland. States are eager to exercise that global power, as their brief to this Court shows. *See*

States Br. 1-3. But it is highly unlikely Congress intended to silently grant it.

Foreign government officers, meanwhile, *are not* "governmental entities" under § 2711(4). So § 2703 makes no provision for foreign-government access to emails. That omission signals that Congress expected that *domestic* authorities would be able to obtain *domestic* communications by serving *domestic* warrants issued by *domestic* courts. Had Congress meant for the SCA to reach emails stored abroad, however, it is "reasonable to conclude" that it "would have addressed the subject of conflicts with foreign laws and procedures" by addressing whether and how to accommodate foreign governments' needs. *Aramco*, 499 U.S. at 256.

This omission grew even starker when Congress amended the SCA to address foreign governments' access to communications in 2009. By then, the internet was a global phenomenon. Yet, as discussed above (at 18), the amendments addressed only foreign governments' access to emails stored in the United States. Congress still did not address foreign governments' access to emails stored *in foreign countries*. That must mean Congress assumed the SCA does not reach them. "In short, foreign law alone, not United States law, currently governs" emails stored abroad. *Microsoft*, 550 U.S. at 456.

Second, while "the presence of an officer [is] not … required for … execution of a search warrant" under § 2703(g), executing warrants in the standard way is not prohibited, either. Indeed, the warrant here declared to "Any authorized law enforcement officer":

"YOU ARE COMMANDED to execute this warrant." J.A. 22. If § 2703 authorized warrants for emails stored abroad, Congress would have explicitly prohibited law-enforcement officers from executing warrants themselves for data stored overseas. *See infra* at 36-37.

Third, § 2703 does not read like a provision directed at affirmatively enhancing the Government's access to electronic communications. It does not grant the Government a power to compel disclosure of all electronic communications possessed by anyone anywhere (*e.g.*, on an individual or company's private computer). It regulates disclosures of the much smaller universe of emails held in storage by service providers—the third-party custodians that customers entrust to keep their communications confidential.

Morrison found such context important to the focus inquiry. This Court observed that "Section 10(b) [of the Exchange Act] does not punish deceptive conduct, but only deceptive conduct 'in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered.'" 561 U.S. at 266. Likewise, § 2703's regulation of the "disclosure" of communications to law enforcement is limited to those "electronic communication[s] … in electronic storage."

b. The Government does not address any of this. Instead it fixates on the ultimate "disclosure" that comes at the end of the process mandated by § 2703. It characterizes what precedes that disclosure as merely "gather[ing] any responsive materials in the provider's control." Br. 36. But the SCA does not refer

to that critical first step in such bland terms. It characterizes what Microsoft does in that step as the "execution of a search warrant." § 2703(g).

The Government observes (Br. 23) that Congress used variants of the word disclose "a dozen times throughout [§ 2703.]" But Congress did so to carve out specific exceptions to § 2702's broad prohibition against the "disclosure of customer communications or records." Repeating "disclosure" in § 2703 was necessary for those exceptions to dovetail with § 2702. It did not, however, modify the meaning of "warrant." "Disclosure" is not the object of the statute's solicitude; rather, it is merely the final step in the chain of actions a provider must take to "divulge" to a governmental entity *whatever* protected material is yielded by the legal instrument specified, whether a warrant, a subpoena, or § 2703(d) order. § 2702(b)(2).

The Government further errs in emphasizing (Br. 24) that the PATRIOT Act amendment added the term "disclosure" to the SCA's section headings, while ignoring the much more salient feature of that amendment: Congress's repeated statements that warrants issued under § 2703 reach only "nationwide," not worldwide. *See supra* at 17.

3. A focus on "disclosure" would have left gaps in coverage in 1986 that are inconsistent with Congress's clear intention.

At minimum, Congress wanted to assure U.S. citizens that the private correspondence they entrusted to service providers for storage in the United States

would be protected from unauthorized intrusion. The Government's reading of the statute "lead[s] to strange gaps in … coverage" by denying that basic level of protection. *RJR Nabisco*, 136 S. Ct. at 2104.

Assume the Government is correct (Br. 13) that the SCA's focus is "disclosure." That means it regulates domestic disclosures only. Now imagine that, back in 1986, a U.S. service provider (or rogue employee) breached a customer's trust and mailed a copy of a U.S. citizen's U.S.-stored emails to a tabloid in London—or to a foreign government. On the Government's theory, there would have been no violation of § 2702's ban on voluntary disclosure, because the disclosure occurred abroad. That cannot be right—and could not have been right in 1986—because the scenario strikes at the very core of what we know Congress wanted to protect.

The Government has not pointed to any comparable incongruity arising from our reading—that Congress's focus *in 1986* was on the security of communications in storage. Instead, the Government points to potential gaps in coverage that arose decades after Congress wrote the statute, with the rise of the global internet. They are all irrelevant, because *Morrison* prohibits attempts to "'discern' whether Congress would have wanted the statute to apply" to circumstances it did not envision. 561 U.S. at 255.

For example, the Government posits that Congress would not have condoned a situation where "a U.S. provider doing business in the United States need not disclose an email about a crime in the United States, even though that email can be retrieved [from

overseas] by the U.S. provider at its U.S. offices." Br. 42. The Government also speculates that Congress would not have approved a process "that a U.S. provider could nullify by the expedient of shifting data to storage devices that it locates over the border." Br. 43. We address the Government's overstated policy concerns below (at 54-61). For present purposes, suffice it to say that we don't know what Congress would have thought, because Congress did not imagine in 1986 that these scenarios were even possible. All we know is that Congress never authorized what the Government's reading of the SCA allows: the unilateral authority to seize foreign citizens' private communications about foreign matters stored in foreign lands under the protection of foreign law.

But suppose Congress had looked into the future. It might have been equally troubled by the problems now created by the Government's reading:

- A provider succumbs to demands of the Chinese Ministry of Public Security to remotely access a U.S. server from Beijing and disclose emails of a U.S. citizen—but § 2702 would not prohibit the disclosure (and the provider would not face liability under § 2707) because the disclosure is in China.

- A hacker in London remotely accesses a U.S. server and supplies a U.S. citizen's emails to a British tabloid—but the hacker cannot be prosecuted under the SCA because he accessed the U.S. server from London.

- A wannabe "America's Toughest Sheriff" sparks an international incident by descending on the Silicon Valley office of the Chinese cloud-computing giant Alibaba with a warrant demanding that it reach into a server in Beijing to retrieve a Chinese official's correspondence with party leaders—insisting the warrant is legal because the disclosure would be in the United States.

These are precisely the sorts of competing concerns that require nuanced legislation—not judicial speculation about the intent of a legislature that never imagined them. Precisely because Congress never accounted for the possibility that providers could sit in one country and access emails stored in another, *either* interpretation will inevitably yield some gap in coverage in the digital era. That is why everyone agrees that Congress should update the SCA. Until then, this Court should stick to the statute that Congress actually wrote: one that governs only electronic communications stored here.

B. The conduct that the SCA compels is a law-enforcement seizure, which occurs where the private correspondence is stored.

Stepping back from the sometimes-abstract exercise of divining Congress's "focus," it helps, at *Morrison*'s second step, to consider the actual conduct that the statute's text commands and assess where it occurs. Section 2703 requires providers to assist the Government with the "execution of a search warrant." § 2703(g). As part of executing a warrant under

§ 2703, law enforcement generally outsources to the provider the task of "searching for, assembling, [and] reproducing" the protected communications from electronic storage on the Government's behalf. § 2706(a).

Any warrant is executed *in* the place to be searched. A search warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Here, the "searching for, assembling, [and] reproducing" all occur in Ireland. The relevant act is the same as if U.S. agents bearing a warrant directed Hilton to send a housekeeper into a hotel room in Dublin, photograph a guest's papers, and email the copies to Washington. It is the execution of a search warrant in a place outside the United States.

1. For purposes of determining the location of the relevant act, it does not matter that Microsoft, rather than the Government, would search for, copy, and import the target electronic communications. Where a private party acts "by compulsion of sovereign authority," the search or seizure is "attributable to the Government." *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614-15 (1989).

The Government cites (Br. 29-30) *California Bankers Ass'n v. Shultz*, 416 U.S. 21, 52 (1974), which held that a bank does not effect a seizure when, pursuant to federal record-keeping requirements, it maintains and produces records of transactions to which it is a party. But the SCA's raison d'être was to treat emails like the contents of a safe-deposit box that a bank holds for safekeeping—which would require a search warrant to obtain—*not* like the bank's

own transaction records. *See supra* at 4-6. The Government also suggests (Br. 30) that "a person who complies with a subpoena" cannot "become[] a government agent simply by collecting and producing evidence in its possession." But demands for email content involve execution of *warrants*, not subpoenas. *See infra* at 44-51.

The Government is similarly wrong to contend (Br. 27) that the overseas steps of copying and "transferring data from its servers in Ireland" are irrelevant because Microsoft could, theoretically, "mov[e] a user's data to another server here or abroad" "at will." There is a world of difference between what a private party is permitted to do under its contract with another private party and what it does by Government command. *See, e.g.*, *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The Hilton housekeeper could enter your hotel room and tidy your papers left on the desk, but it is still a search and seizure when the Government compels her to photograph them. *See Warshak*, 631 F.3d at 287. Here, the Government is demanding that Microsoft move a customer's digital property somewhere it would not be in the normal course of business. The only authority the Government has invoked to order Microsoft to import those emails from Ireland is § 2703. That compelled conduct is central, not incidental, to the statute's operation. Moreover, the Government's reading of the SCA would allow it to order the transfer of foreign customers' foreign-stored communications to the United States, even when an account owner has specified that the provider must *not* move them. *See* U.S. Chamber of Commerce Br. (observing that corporate customers impose such requirements).

2. It also does not matter that the warrant here targets digital, rather than paper, letters. While "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." Pet. App. 21a. And collecting private communications, including in electronic form, constitutes a search and seizure. *See United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297, 313 (1972); *Katz v. United States*, 389 U.S. 347, 354 (1967). "Of course, the framers were concerned with the protection of physical rather than virtual correspondence," but when the Government copies and searches private email content, that "pretty clearly … qualif[ies] as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *United States v. Ackerman*, 831 F.3d 1292, 1307-08 (10th Cir. 2016) (Gorsuch, J.).

The Government contends that "transfer[ing] information from [the] datacenter in Dublin to [Microsoft's] offices in the United States" does not "interfere[] with a user's possessory interests." Br. 31. But courts uniformly agree that copying electronic data effects a seizure. Pet. App. 43a-44a; *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1168-69 (9th Cir. 2010) (en banc); *Warshak*, 631 F.3d at 282-84; *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002). Federal Rule of Criminal Procedure 41(e)(2)(B) likewise equates the "on-site copying" of "electronically stored information" with a "seizure." Even before any government agent takes a

peek, copying someone else's otherwise-private papers (whether digital or physical) for law-enforcement purposes interferes with one of an owner's most important property rights: "the right to exclude others." *See, e.g.*, *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978).

3. The Government points out (Br. 25) that the search and seizure here would be effected remotely, without any "deployment of American law enforcement personnel abroad." But a remote search is still a search of the distant locale: When police access information from a smartphone on the street "at the tap of a screen," "a search of files stored in the cloud" occurs on the "remote server," not the street. *Riley*, 134 S. Ct. at 2491. Similarly, when a law-enforcement agent points a thermal-imaging sensor at a house "from the passenger seat of [his] vehicle across the street," the search is in the house, not in the car or the exterior wall. *Kyllo v. United States*, 533 U.S. 27, 30, 35 & n.2 (2001).

So too here. If federal agents sitting in Washington remotely access a computer located in a foreign country, copy data stored on that computer, and import it, the search and seizure occurs in the foreign country and not in the United States. The Government has successfully argued just that elsewhere, in order to avoid complying with the Fourth Amendment's warrant requirement for such searches and seizures. *See United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001). Warrants issued under the SCA are no different: Congress explained that the SCA's provisions

"are intended to apply only to access within the territorial United States." H.R. Rep. No. 99-647, at 32-33.

***

At bottom, the Government contorts the "focus" inquiry to ignore the significant, intrusive law-enforcement activity abroad in favor of the mechanical steps that bookend it in the United States—what the Government calls "inputting commands at [Microsoft's] facility in the United States" and the subsequent "domestic disclosure of information to the government." Br. 26. But no one describes air travel as a road trip just because it involves taxiing to and from the runway. As *Morrison* explained, "the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case." 561 U.S. at 266. Because the Government seeks to use the SCA to compel Microsoft's assistance in conducting a seizure of emails stored in Ireland, the conduct relevant to the statute's focus occurs there.

C. The international discord that has erupted, and the potential for conflict with foreign laws, confirm that the warrant entails an impermissible extraterritorial application of the SCA.

1. In "evaluating the 'relevant' conduct" under the presumption against extraterritoriality, courts are properly "mindful" of this Court's "emphasis on … potential foreign policy implications." *Mastafa v. Chevron Corp.*, 770 F.3d 170, 187 (2d Cir. 2014). The

international reaction to this case buttresses the conclusion that it involves an impermissible extraterritorial application of the SCA. The warrant has already yielded precisely the "unintended clashes" between U.S. and foreign law and "international discord" that the presumption against extraterritoriality guards against. *Aramco*, 499 U.S. at 248.

Foreign sovereigns protested when the magistrate judge ordered Microsoft to retrieve emails stored in Ireland. The European Union Commissioner for Justice objected that the order "bypasses existing formal procedures that are agreed between the EU and the US, such as the [MLAT], that manage foreign government requests for access to information and ensure certain safeguards in terms of data protection." J.A. 65-66. She added: "[T]he extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union." *Id.* at 66.

Similarly, Members of the European Parliament, and the Government of Ireland itself, pronounced that executing the warrant would implicate foreign sovereignty. *See* Ireland Br. 1 (asserting Ireland's "genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its territory"); European Parliament Members Br. § II ("[D]irect access by U.S. authorities of personal data stored in the EU (which is what the warrant in this case would permit) would effectively result in the protections afforded by EU law being sidestepped and create a conflict with EU

law.").[3] And foreign newspapers howled, "US Wants to Rule over All Servers Globally." J.A. 68-69; *see also* J.A. 70-111.

This outcry is unsurprising. The United States would be outraged if, for example, Chinese officers investigating leaks to the foreign press descended on a service provider in Beijing with a warrant commanding it to access the emails of a U.S. reporter stored in the United States.

Americans would view that just as our European counterparts have: as an affront to the "basic premise of our legal system that" each country's "law governs domestically but does not rule the world." *RJR Nabisco*, 136 S. Ct. at 2100 (quoting *Microsoft*, 550 U.S. at 454). Under international law, a "state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state," particularly with respect to "criminal investigation[s]." Restatement (Third) of the Foreign Relations Law of the United States § 432(2) & cmt. b. If ever there were a step that is sure to anger allies, it

---

[3] The Government misreads (Br. 47) Ireland's Second Circuit brief to claim that "Ireland possesses the raw power" that the Government now seeks. In the Second Circuit and before this Court, Ireland merely explained that "*in the absence of alternative means* of obtaining information," it recognizes "in certain circumstances" a limited version of the *Marc Rich* doctrine (discussed *infra* at 44-51), permitting domestic process to reach a company's own business records stored overseas, *not* personal documents entrusted to a caretaker. Ireland Br. 5, 7. Contrary to the Government's reading, Ireland urges that "the judgment [of the Second Circuit] be affirmed." *Id.* at 8.

is sidestepping the established government-to-government processes for obtaining evidence located in another country. *See Empagran*, 542 U.S. at 164.

All this illustrates the wisdom of the presumption against projecting U.S. laws into other countries. And it shows why "[i]t has been a maxim of statutory construction since the decision in *Murray v. The Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804), that 'an act of congress ought never to be construed to violate the law of nations, if any other possible construction remains.'" *Weinberger v. Rossi*, 456 U.S. 25, 32 (1982)).

2. "Although 'a risk of conflict between the American statute and a foreign law' is not a prerequisite for applying the presumption against extraterritoriality, where such a risk is evident, the need to enforce the presumption is at its apex." *RJR Nabisco*, 136 S. Ct. at 2107. The Government assures the Court (Br. 50) that the "fear" of "conflicting obligations" "is speculative." But it has told Congress that, "when U.S. authorities are seeking data overseas," there is at least the "potential for conflicts." *Law Enforcement Access to Data Stored Across Borders: Hearing Before the S. Subcomm. on Crime and Terrorism* (May 24, 2017), at 50:30-51:40, https://perma.cc/6GME-GXCH (testimony of Brad Wiegmann, Deputy Assistant Att'y Gen., U.S. Dep't of Justice). And it directs its prosecutors that even subpoenas for records located abroad "can adversely affect" the United States' "relationship with a foreign country," so they may not issue such a subpoena without prior written approval from the Office of International Affairs. U.S. Dep't of Justice,

U.S. Attorneys' Manual, Criminal Resource Manual § 279.B, https://perma.cc/3SYM-7VJ7.

This case presents more than just potential for conflicts. The Government's expansive reading of the SCA will inevitably create conflicts with the laws of other nations. *See* New Zealand Br. 13-14. Take EU law, for example. The European Commission has told this Court (Br. 5-6) that "[t]here is … no doubt that the European Union is actively regulating … how data stored in the European Union must be protected and when such data may be transmitted abroad." EU law governs what the warrant here directs: the "collection … and transfer of personal data" stored in Europe. *Id.* at 8. And in most cases, EU law *prohibits* the transfer of personal data out of the European Union in response to a unilateral demand from a foreign government. Article 48 of the European Union's General Data Protection Regulation (GDPR), which takes effect in May 2018, commands that an MLAT must be used in the ordinary course: "Any judgment of a court … requiring a [provider] to transfer or disclose personal data may *only* be recognised or enforceable in any manner *if based on an international agreement*," with limited exceptions. Commission Regulation 2016/679, art. 48, 2016 O.J. (L 119) 64 (emphases added).

Thus, according to the European Commission (Br. 14), EU law "makes clear that a foreign court order" like the one here "does not, as such, make a transfer lawful under the GDPR." The college of the 28 national authorities responsible for interpreting and enforcing the GDPR is even clearer: Upon "the Supreme Court decision to review … the Microsoft warrant

case," it "t[oo]k[] the opportunity to remind that, in line with Article 48 of the GDPR, … circumvention of existing MLATs or other applicable legal basis under EU law by a third country's law enforcement authority is … an interference with the territorial sovereignty of an EU member state." *Statement of the Art. 29 Working Party*, 9 (Nov. 29, 2017), https://perma.cc/5EM2-7F9K.

The Government has nevertheless asserted (Cert. Reply Br. 8 n.2) that because Article 48's prohibitions are "without prejudice to other grounds for transfer," the GDPR's exceptions will permit compliance with unilateral U.S. warrants. But there is no blanket exception that would permit transfers of the sort contemplated here. As the European Commission confirms (Br. 15-16), the exceptions that do exist require case-by-case assessments of the nature of the foreign request for data and must be "strictly" construed under EU law. Br. 16. Ireland's enforcement agency, for example, has announced that in its view the EU's "public interest" exception is "only likely to be relevant to *public sector* data controllers and only in circumstances where they can show that there is a substantial *Irish* public interest in the transfer of personal data"—so it would not apply here. Ireland Data Protection Commissioner, *Transfers Abroad*, https://perma.cc/96V2-MHNW (emphases added). Providers would be left to guess ahead of time whether they would ultimately be able to prove to foreign authorities that a given transfer fits within a narrow exception. The penalty for guessing wrong could be devastating: up to 4% of a company's *worldwide revenues*. European Commission Br. 12. That is $3.6 *billion* for Microsoft.

Besides, the Government's interpretation of the SCA would authorize *all* demands for foreign-stored data by federal, state, and local law enforcement, regardless of whether EU or other foreign law permits the provider to comply in that instance. In other words, the Government's reading of the SCA would systematically ignore other sovereigns' interests in regulating the scope of foreign-government access to data stored within their territory.

The Government also contends that its expansive reading of the SCA is necessary to "compl[y] with [U.S.] treaty obligations." Br. 47-49. It claims that the Budapest Convention requires signatories to adopt legislation creating unilateral data-access powers, and that because Congress never enacted such legislation, § 2703 must already have qualified. But the Convention does not require signatories to enact the kind of expansive powers the Government now seeks. In fact, the signatories rejected requiring broad unilateral access to content data stored in other countries. *See* Extraterritorial and International Law Scholars Br. § I.C.1. Moreover, the Senate's unicameral ratification of the Convention pursuant to its Treaty Power in 2006 is irrelevant to the meaning of the SCA—which *Congress* enacted 20 years earlier.

The presumption against extraterritoriality entrusts to Congress alone the prerogative to determine whether and in what circumstances the United States will assume the risks from reaching into foreign sovereign nations, even remotely, to conduct criminal investigations. Because Congress has not exercised that prerogative, the Government cannot order Microsoft

to import electronic communications from the foreign country where they are stored.

III. Pre-*Morrison* Cases Addressing A Subpoena's Global Reach Shed No Light On The Focus Of The SCA's Warrant Provision.

With scant textual support for its position on the SCA's focus, the Government resorts to the interpretive equivalent of a four-rail bank shot. Its reasoning (Br. 32-36) is complicated:

1. There is a line of lower-court cases about the reach of *subpoenas*, exemplified by *Marc Rich & Co. v. United States*, 707 F.2d 663 (2d Cir. 1983), holding that a company receiving a subpoena for *its own business records* may not "resist the production of documents on the ground that the documents are located abroad." *Id.* at 667.

2. This principle should also extend not just to a company's own business records but to private papers that customers entrust to the company for safekeeping.

3. Congress must have had such an extension of *Marc Rich* in mind when it crafted the SCA.

4. That must mean that Congress wanted *warrants* issued under the SCA to also reach customer's emails stored overseas.

As an initial matter, this reads like a *Morrison*-step-one argument that Congress intended the SCA

to have extraterritorial reach—which the Government concedes it did not. To the extent this argument has any bearing on whether Congress's focus was on disclosure or storage, it fails. As the Court of Appeals recognized, this reasoning is at war with the SCA's text. Pet. App. 30a-32a. And the Government inaccurately portrays the legal backdrop in any event.

A. Conflicts with the SCA's text erupt at every stage of the Government's subpoena argument.

First, "[w]arrants and subpoenas are, and have long been, distinct legal instruments." Pet. App. 31a. Far from blurring that age-old distinction, the SCA explicitly adopts it: Section 2703(a) requires a "warrant" for the Government to obtain individuals' private electronic communications. In contrast, subsection (c) authorizes the Government to obtain less sensitive information, like subscriber information or a "network address," via "an administrative subpoena … or a Federal or State grand jury or trial subpoena." § 2703(c)(2). There is no reason to think that Congress intended to incorporate the geographic breadth of a subpoena when it used the distinctly territorial term "warrant." *See supra* at 15.

Second, the Government repeatedly characterizes emails as producible "records" akin to a company's own business records. *E.g.*, Br. 16, 22, 32. But the SCA defines "records" as "*not including* the contents of communications." §§ 2702(c), 2703(c) (emphasis added). Congress crafted separate "warrant" and "subpoena" provisions precisely because it wanted to ensure that email content was *not* treated like a "bank's … records," which are accessible by subpoena.

H.R. Rep. No. 99-647, at 23 n.41; *see* S. Rep. No. 99-541, at 3, 38. Instead, Congress viewed email content as "analogous to items stored, *under the customer's control*, in a safety deposit box," not to documents in the *provider's* possession, custody, or control. H.R. Rep. No. 99-647, at 23 n.41 (emphasis added); *see supra* at 4-6.

Earlier this Term, the Government embraced this very distinction. It assured this Court that email content is comparable to a paper letter in a sealed envelope. Thus, it conceded that "individuals who rely on a third party to deliver their communications do not thereby lose an expectation of privacy in the contents of those communications," unlike the provider's records of transactions with its customers. Brief for United States, *Carpenter v. United States*, No. 16-402, at 36-37(U.S. Sept. 25, 2017); *see also id.* at 36-38, 45-46; Transcript of Oral Argument at 45, *Carpenter v. United States*, No. 16-402 (U.S. Nov. 29, 2017) (hereinafter "*Carpenter* Tr.").

Third, § 2703(a) formulates the service provider's obligation with words that bear no resemblance to the compelled-production rules the Government invokes. Such provisions typically speak of materials "in the responding party's possession, custody, or control," *e.g.*, Fed. R. Civ. P. 34(a)(1), 45(a)(1)(A)(iii); Fed. R. Crim. P. 16(a)(1), (b)(1), or more generally of "producing" documents, *e.g.*, Fed. R. Crim. P. 17(c); 18 U.S.C. § 3486. Section 2703, in contrast, never mentions either. Instead, it names the specific place where target communications must be found—"in electronic storage."

Fourth, the text also contradicts the Government's argument (Br. 36) that "the execution of a Section 2703 warrant … functions like the execution of a subpoena." The Government contends (Br. 36) both are "served … by transmitting the demand for disclosure to a provider," who must then "gather any responsive materials in the provider's control" without the presence of an officer. The Government cites § 2703(g) for that equivalence. But § 2703(g) expressly confirms that what the provider is doing is the "execution of a search warrant." It merely prescribes one difference from a traditional warrant—that a law-enforcement officer need not be present. *See United States v. Bach*, 310 F.3d at 1066 n.1; H.R. Rep. No. 107-497, at 79-80 (2002). Just because *one* aspect of executing a warrant under § 2703 resembles serving a subpoena does not mean that a § 2703 "warrant" should be treated like a subpoena in all *other* respects, including the *Marc Rich* rule.[4]

Fifth, the Government's argument (Br. 29-30) that a "warrant" under § 2703(a) is just a probable-cause subpoena retreads the District Court's reasoning that the SCA creates "a hybrid: part search warrant and part subpoena." Pet. App. 84a; *see* Pet. App. 100a. But Congress demonstrated that if it wanted to create a "hybrid" instrument, it did so explicitly, as it

[4] The Government overreads (Br. 36-37) a 2001 amendment. Section 2703(a) originally required that warrants be issued "under" Rule 41. The amendment altered the language of § 2703(a) to provide that SCA warrants are issued "using the procedures described in" Rule 41. That amendment simply implemented the contemporaneous change allowing a § 2703 warrant (unlike a Rule 41 warrant) to reach *nationwide*. *See supra* at 17. But it did nothing to alter the way SCA warrants are *executed*.

did in § 2703(d). And from the *account owner's* perspective, the execution of a § 2703 warrant looks exactly like the execution of a warrant: It comes by surprise. That is why the Government is wrong to suggest (Br. 37) that the availability of a pre-enforcement challenge shows that SCA warrants are effectively subpoenas. *Compare Donovan v. Lone Star Steer, Inc.*, 464 U.S. 408, 414 (1984); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946). The *target* has no pre-execution opportunity to move to quash. The only reason a provider can challenge the warrant is that § 2703 allows the Government to co-opt the provider to help execute the warrant.

B. The Government is also mistaken in drawing support for its position from the SCA's structure. The crux of the Government's argument is that § 2703 operates as an "upside-down pyramid" with more protective processes (like warrants) able to do everything that less protective devices (like subpoenas) can do and more. Br. 4. True, the *types of information* that a warrant or a subpoena can demand fit that hierarchy: A warrant can be used to demand any information that can be sought with a subpoena. § 2703(b), (c). But that does not mean the *procedural trappings* of each nest in the same way. Clearly they do not: Warrants must describe with particularity the location to be searched, whereas subpoenas can order the production of records irrespective of where they are kept. In any event, like most of the Government's arguments about congressional intent, any incongruity here is merely a consequence of subsequent technological developments Congress never imagined. As to domestically stored communications (which is all Congress contemplated in 1986), warrants, § 2703(d) orders,

and subpoenas nest precisely as the Government suggests they should.

Equally anachronistic is the Government's related argument (Br. 39-40) that limiting the reach of SCA warrants to domestically stored content would result in a "bizarre bifurcation of the statute." That argument starts from the premise that subpoenas for emails older than 180 days would reach abroad. But email content can *never* be obtained by subpoena: The statute's archaic 180-day distinction has no force after *Warshak*, 631 F.3d 266. Not only has the Government acquiesced in that holding, *see supra* at 6 n.1; H.R. Rep. No. 99-647, at 68, 72 (explaining the now-outdated justification for the six-month rule), its recent concession to this Court, discussed above (at 46), embraces *Warshak*'s central premise—that customers retain a reasonable expectation of privacy in *all* of their emails even when entrusted to a service provider.

C. Even if the Government could overcome the lack of textual and structural support for importing subpoena rules into warrants, the argument would still fail for two reasons.

First, the Government's premise is that Congress legislated against the "backdrop of settled law." Br. 32-34. But no court has ever extended *Marc Rich* to allow a subpoena to reach private papers that a cus-

todian holds in trust for a customer in another country.[5] So there is no reason Congress would have assumed that subpoenas had that power. The "backdrop" the Government describes is a blank scrim. What the Government actually seeks here is an unprecedented—and intrusive—expansion of the *Marc Rich* line of cases.

Second, this Court has never endorsed the *Marc Rich* doctrine.[6] And that doctrine is difficult to square with *Morrison*, which itself set aside a line of cases developed "over many decades" in "various courts of appeals" that similarly required district courts to conduct case-by-case, multifactor balancing. 561 U.S. at 255. Whatever *Marc Rich*'s validity, this Court should not *extend* it to require a custodian to seize a customer's most intimate private correspondence held in trust in another country. Even the traditional application of *Marc Rich* is fraught with the potential for

---

[5] Even domestically, there is negligible support for the view that a subpoena to a mere custodian can reach private papers held in trust for a customer. The Government cites (Br. 40-41) *In re Horowitz*, 482 F.2d 72, 73 (2d Cir. 1973) and *Fisher v. United State*s, 425 U.S. 391 (1976). But in *Horowitz*, the court allowed the subpoena to reach only business records the client openly exposed to his accountant, while quashing the subpoena to the extent it sought the client's personal documents and letters. 482 F.2d at 75 & n.2. And *Fisher* did not involve private papers at all. 425 U.S. at 414.

[6] The Government cites *Société Nationale Industrielle Aérospatiale v. United States District Court*, 482 U.S. 522, 540-41 (1987), but it does not contend that *Aerospatiale* embraced the *Marc Rich* rule. *Aerospatiale* addressed only a *civil litigant*'s *own business records*—not a third-party subpoena—and it held only that the Hague Convention did not entirely displace ordinary discovery procedures under the Federal Rules of Civil Procedure.

conflict: "No aspect of the extension of the American legal system beyond [our borders] has given rise to so much friction as the requests for documents in investigation and litigation." Restatement (Third) of Foreign Relations Law § 442. The international ramifications of executing a warrant for a customer's private correspondence are much more serious. *Cf. Oklahoma Press Pub. Co.*, 327 U.S. at 208 (recognizing that subpoenas are less intrusive when they seek only corporate records). This Court should not ascribe to Congress an unstated intention to authorize a significantly greater intrusion on sovereignty than any court has allowed before.

The international friction will only escalate as individuals, companies, and governments store more private information in the cloud. As with smartphones, "there is an element of pervasiveness that characterizes" emails and cloud-based storage. *Riley*, 134 S. Ct. at 2490. The justifications for a pre-internet doctrine allowing worldwide compelled production of a company's "business information," *United States v. First Nat'l City Bank*, 396 F.2d 897, 901 (2d Cir. 1968), simply do not translate to the "sensitive records[,] previously found in the home," that citizens of every nation now store in the cloud. *Riley*, 134 S. Ct. at 2491. "[A]ny extension of that reasoning to digital data has to rest on its own bottom." *Id.* at 2489. And the Government's proposed expansion does not.

IV. The Government's Policy Concerns Are Properly Addressed To Congress.

A. The Government warns of "[d]etrimental" practical consequences if the SCA does not reach data

stored overseas. Br. 41-45. But this is not the forum to address those concerns. Everyone agrees that the SCA is "badly outdated" and must be revised to account for today's "globally-connected" era. Pet. App. 49a (Lynch, J., concurring). Yet Congress "alone has the facilities necessary to make fairly such an important policy decision where the possibilities of international discord are so evident and retaliative action so certain." *Benz v. Compania Naviera Hidlago, S.A.*, 353 U.S. 138, 147 (1957). That is why the presumption against extraterritoriality preserves Congress's prerogative to decide whether and how a statute should be extended abroad. Pet. App. 14a; *see* Members of Congress Br. § 1.

The Government has already presented Congress with a draft bill for the very purpose of responding to the decision below. Letter from Samuel R. Ramer, Acting Assistant Att'y Gen., U.S. Dep't of Justice, to Hon. Paul Ryan, Speaker, U.S. House of Reps., at A1 (May 24, 2017), https://perma.cc/MUT6-A8GC ("Ramer letter"). Meanwhile, a bipartisan group of Senators and Representatives is advancing another, more balanced proposal, the International Communications Privacy Act (ICPA). S. 1671, 115th Cong. (2017).

Unlike in other arenas, there is every reason to expect that Congress will act. As the Government recently observed, "Congress has been active in this area." *Carpenter* Tr., *supra*, 49. Just eight years ago, Congress amended the SCA to facilitate cross-border data transfers under cooperative agreements. *Supra* at 18. When the Department of Justice urges Congress to address a law-enforcement issue,

Congress takes action—even if it does not give law enforcement everything it seeks.

The competing legislative proposals illustrate the folly in judicial efforts to use the tools of statutory interpretation to solve an international problem that Congress has not yet tackled. Unlike Congress, this Court has an unsatisfactory "all-or-nothing choice": Either *all* local, state, and federal law-enforcement officers can use the SCA to demand *all* communications stored abroad; or *no* officer can demand *any*. Pet. App. 69a (Lynch, J., concurring). Congress, in contrast, can "balanc[e] the needs of law enforcement … against the interests of other sovereign nations" and the privacy and economic consequences of allowing law enforcement to use U.S. warrants to reach into foreign countries. Pet. App. 68a, 69a, 72a (Lynch, J., concurring). The bipartisan ICPA proposal, for example, would authorize law enforcement to obtain emails belonging to "United States person[s]" and persons "physically located [in] the United States," regardless of where those emails are stored. S. 1671, 115th Cong. § 3. But it does not grant the same access to emails of foreigners. No such policy compromise is available to this Court interpreting the current statute.[7]

---

[7] Contrary to the Government's suggestion (Br. 51-52 & n.5), nothing in the current statute allows courts to craft any exemption for providers who face "competing foreign obligations" and make "good faith effort[s] to secure permission from the foreign authorities," or for scenarios implicating "legitimate interests of the foreign sovereign with respect to its law." This Court has recognized that it "is too complex to" expect courts to "take … account of comity considerations case by case." *Empagran*,

History confirms that, when courts stay their hand, Congress does step in. In *Aramco*, for example, this Court properly declined to imagine whether Congress would have wanted Title VII of the Civil Rights Act to apply abroad, inviting Congress to step in. *Aramco*, 499 U.S. at 255. Congress promptly amended the statute to apply extraterritorially, but only in carefully tailored circumstances. *See* Civil Rights Act of 1991, Pub. L. No. 102-166, 105 Stat. 1071, 1077. The presumption thus "provoked Congress into providing just the sort of nuanced specificity and limitations that the Court would have had difficulty divining." Einer Elhauge, *Statutory Default Rules: How to Interpret Unclear Legislation* 206 (2008).

B. Even if this were the right forum to consider the Government's practical concerns, its policy analysis is flawed and incomplete.

The Government's main theme is to lament the lost opportunity to reach foreign-stored communications. But when Congress wrote the SCA, the Government could not have obtained the huge volume of personal correspondence it now can, even with a warrant. It would have had to locate and seize those communications envelope by envelope and filing cabinet by filing cabinet. And when the target kept those envelopes and files in other countries, the Government

---

542 U.S. at 168; *compare* E-Discovery Inst. Br. § III (proposing such a new analysis). But even if that approach were more attractive, only Congress can decide whether to burden district courts with assessing in each case the substance and potential penalties of complex and novel foreign data-privacy laws.

had to engage with foreign governments through MLATs and cooperative efforts.

In the years since, cloud storage has facilitated law-enforcement investigations—and increased the potential for law-enforcement abuse—more than any technological development in recent memory. Caches of personal information and correspondence of a scope previously unimaginable are now available on demand. When that information is stored in the United States—as it is for most crimes the Government investigates—the SCA is a formidable investigative tool. But just because it has recently become technologically possible to reach a similar cache of private correspondence stored in foreign lands does not mean it is legal or prudent to do so. Congress could decide to expand the Government's access to private correspondence stored exclusively abroad. But until it does, the Government has to make do with the many other formidable tools that have served it well until now.

We noted above (at 30-32) some of the Government's other, more specific complaints: that Congress would not have wanted to "hamper" U.S. law-enforcement efforts by allowing providers the "choice" to store data overseas. Elsewhere it asserts "that a U.S. provider" should not be allowed to "nullify [the Government's access] by the expedient of shifting data to storage devices that it locates over the border." Br. 43. But that is like saying a U.S. company whose shares trade on a foreign exchange should be subject to a securities-fraud suit in U.S. court, notwithstanding *Morrison*, because the company "chose" to list them

there. To the contrary, the presumption against extraterritoriality takes statutes, and businesses, as it finds them.

In any event, Microsoft's decision where to store a customer's emails is not some "expedient" designed to "hamper" law enforcement. Business imperatives dictate Microsoft's storage decisions. No customer likes to wait for a webpage to load when she wants to read her emails. Microsoft avoids such delays by storing emails physically near the customer. That means "the email[s] [of] a U.S. citizen living in the United States," Gov't Br. 42, are stored here and *would* be subject to seizure under a valid warrant. Conversely, foreign customers reasonably expect—and foreign businesses increasingly demand—that their private data be stored in a nearby location where local law protects it.

The Government protests that the decision below "provides a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement." Br. 42 (quoting Pet. App. 126a). That is absurd. The Government's reading of the SCA does not prevent criminals from evading the reach of U.S. warrants. Any criminal bent on eluding U.S. warrants can use an entirely foreign email provider that U.S. law enforcement could *never* access. ProtonMail, for example, promises to keep users' emails locked away in Switzerland—"outside of US and EU jurisdiction"—using end-to-end encryption intended to stymie *any* law-enforcement investigation. ProtonMail, *Security*, https://perma.cc/C2MF-5HZQ. To the extent that criminals read Supreme Court briefs for roadmaps,

the Government's rule plots a course straight to services like ProtonMail.

Of course, the Government has offered no evidence that anyone in the United States has ever manipulated Microsoft's system in this manner. And if anyone did try that gambit, they would now find that this supposed roadmap leads to a dead end. As part of its ongoing effort to improve service and prevent abuse, Microsoft now automatically detects customers' *actual* location and stores their emails in datacenters nearby. Microsoft, *Delivering a Faster and More Responsive Outlook.com* (Oct. 27, 2017), https://perma.cc/MZ8Y-JT7P.

C. With all its focus on law-enforcement needs, the Government ignores the serious countervailing consequences of its position. Interpreting the current statute to grant any federal, state, or local officer the unfettered power to reach into other nations' territory and seize data stored there would raise the very concerns identified in *Morrison* and *Kiobel*: Such a projection of U.S. law-enforcement power into foreign countries would trammel their sovereignty and threaten to disrupt harmony among nations, most significantly by ignoring carefully negotiated international agreements. *See supra* at 37-43.

The Government's approach also presents an existential threat to the multibillion-dollar U.S. cloud-computing industry. U.S. companies are the world leaders in cloud storage. That lead is built on trust, which has already been shaken by Edward Snowden's revelations about U.S. surveillance. It will evaporate

entirely the moment this Court directs that U.S. companies must disclose emails stored in foreign nations even when doing so would violate the data-privacy laws of those nations. First will go the trust of foreign governments who have been customers. Then foreign businesses will follow, with foreign consumers right behind them. Foreign governments are already preparing for a separation from U.S. technology companies. France, for example, is considering developing "'le cloud souverain'—the sovereign cloud—to limit cloud services in France to French companies operating in France." Former Law-Enforcement Officials Br. 12.

And then there is the issue of Americans' privacy. If this Court declares that unilaterally seizing private correspondence across borders is a purely domestic act, then the United States will have no basis to object when other countries reciprocate and unilaterally demand the emails of U.S. citizens stored in the United States from providers' offices abroad. If we can do it to them, they can do it to us.[8]

---

[8] The Government incorrectly argues (Br. 46) that "no such negative consequences have ensued" in the months since several magistrate and district judges disagreed with the decision below. While this case was pending, Brazil tried to force Microsoft to comply with unilateral orders for data stored in the United States. It levied fines and even arrested and criminally charged a Microsoft employee located in Brazil. *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Judiciary Comm.* (Feb. 25, 2016), https://perma.cc/Z2ZE-PQ8F (testimony of Brad Smith, President and Chief Legal Officer, Microsoft Corp.). These sorts of incursions on American sovereignty would surely increase if

The Government's chief law-enforcement agency is free to argue that the reach and efficiency of its criminal investigations outweighs all these costs and risks. But only Congress can decide whether the tradeoff is worth it.

D. The Government raises other practical concerns involving "other … providers that have different corporate systems for storing data." Br. 43-45. But it discusses only Google, which has litigated—and lost—a series of cases challenging SCA warrants. The Government's inaccurate portrayal of Google's architecture confirms the wisdom of not deciding cases based on facts that are outside the record—and of leaving to Congress the job of investigating and understanding the wide range of factual scenarios in which a policy judgment might play out.

The Government portrays Google's architecture as "splitting a single email into separate pieces" that "constantly move[] … around the world." Br. 45. It says that this makes an account's location at "any given moment in time … difficult or impossible to ascertain," rendering MLATs "futile." Br. 45. But Google never said that—and it is patently wrong. Data *necessarily* has an ascertainable physical location: A computer network must "know" where a customer's data is in order to access it on command. All Google said was that the tool it designed to query its systems

---

the United States Supreme Court were to grant the Government the power it seeks.

when responding to a warrant did not provide its technicians with the specific location of a certain piece of data.

It is no wonder, then, that Google lost the cases it brought: It could not confirm that the communications targeted by search warrants were outside the United States during the entire period that the warrants were valid. *See e.g.*, Hearing Transcript 27, 40, *In re Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-80263 (N.D. Cal. Aug. 10, 2017). Google was thus unable to plead a threshold fact necessary to trigger the presumption against extraterritoriality.

In contrast, the record in *this* case indisputably establishes that predicate fact: The private communications the Government seeks are outside the United States for the long haul. They are stored all together, in a discrete, identifiable location—on a server in a datacenter in Dublin, Ireland—where the information is regulated by Irish data-protection law and subject to the United States-Ireland MLAT.

E. Finally, the Government protests (Br. 44-45) that the MLAT process on which it has relied for decades is less convenient than requiring a provider to execute an SCA warrant. But the record evidence here establishes that Ireland has implemented its MLAT obligations with "highly effective" legislation that is "efficient and well-functioning"; that "urgent requests can be processed in a matter of days"; and that law enforcement have the option of using a "24/7" hotline to ensure the immediate preservation of data. J.A. 49, 119-120, 122.

Whatever frustrations the Government might have with the MLAT process are simply reasons to urge Congress to improve it. Indeed, the Government's pending legislative proposal includes enhancements specific to the United States and United Kingdom's evidence-sharing procedures for electronic data. Ramer Letter, *supra*, at A3; *see* U.K. Br. 11.[9] Frustrations with existing treaty procedures are no basis to usurp Congress's role in deciding whether and when law enforcement should be allowed to act unilaterally in derogation of those obligations.

***

It bears remembering that the SCA itself was enacted as a response to gaps in the Wiretap Act, which was "written in [the] different technological and regulatory era" of the 1960s. H.R. Rep. No. 99-647, at 17, 22-23. The SCA's drafters struck "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement" in light of the new technologies of the 1980s. *Id.* at 19. Here, too, a new Congress will have to revisit that balance in light of today's technologies and global interconnectedness.

---

[9] The United Kingdom unwittingly supports our position in objecting that the decision below harms its ability to ask the U.S. Government and U.S. courts for help seizing emails stored in *other* countries. *See* U.K. Br. 9. In other words, the United Kingdom wants the United States to be an international waystation for private data that one foreign country wants to seize from another foreign country. U.S. courts can play that extraordinary role, but only with Congress's express endorsement. As if to prove the point, the U.K. simultaneously endorses the proposal to enhance the United States-United Kingdom bilateral agreement—which requires Congress's approval.

And whatever statute Congress passes now, it will surely have to revise a generation hence to reflect advances we cannot yet imagine. For now, the presumption against extraterritoriality limits the SCA, and the warrant issued under it, to communications stored on U.S. soil.

CONCLUSION

This Court should affirm the judgment of the Court of Appeals.

Respectfully submitted,

Bradford L. Smith
David M. Howard
John Frank
Julie Brill
Jonathan Palmer
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

James M. Garland
Alexander A. Berengaut
Lauren K. Moxley
COVINGTON & BURLING LLP
850 10th Street, NW
Washington, DC 20001

E. Joshua Rosenkranz
Counsel of Record
Robert M. Loeb
Brian P. Goldman
Evan M. Rose
Hannah Garden-Monheit
Alec Schierenbeck
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000
jrosenkranz@orrick.com

January 11, 2018

APPENDIX

RELEVANT STATUTORY AND REGULATORY PROVISIONS

1. 18 U.S.C. § 1030(e)(2)(B) (current)

§ 1030. Fraud and related activity in connection with computers

***

(e) As used in this section—

***

(2) the term "protected computer" means a computer—

***

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

***

2. 18 U.S.C. § 2701(a), (c) (current)

§ 2701. Unlawful access to stored communications

(a) Offense.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

***

(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

3. 18 U.S.C. § 2702(a)-(c) (current)

§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of

a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications— A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such

communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

***

4. 18 U.S.C. § 2703 (a)-(d), (g) (current)

§ 2703. Required disclosure of customer communications or records

(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 communications 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—

(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.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) 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;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or

other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

***

(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.

5. 18 U.S.C. § 2703(a) (Oct. 26, 2001)

§ 2703. Required disclosure of customer communications or records

(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 by a court with jurisdiction over the offense under investigation or equivalent State warrant. 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 communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

***

6. 18 U.S.C. § 2703(a) (1986)

§ 2703. Requirements for governmental access

(a) Contents of electronic communications in electronic storage.

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

***

7. 18 U.S.C. 2706(a) (current)

§ 2706. Cost Reimbursement

(a) Payment.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

***

8. 18 U.S.C. § 2707(a)-(c) (current)

§ 2707. Civil Action

(a) Cause of action.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

***

9. 18 U.S.C. § 2711(3)-(4) (current)

§ 2711. Definitions for chapter

***

(3) the term "court of competent jurisdiction" includes—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; and

(4) the term "governmental entity" means a department or agency of the United States or any State political subdivision thereof.

10. 18 U.S.C. § 2711(3) (Oct. 26, 2001)

§ 2711. Definitions for chapter

***

(3) the term "court of competent jurisdiction" has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.

***

11. 18 U.S.C. § 3127(2) (Oct. 26, 2001)

§ 3127. Definitions for chapter

***

(2) the term "court of competent jurisdiction" means—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

***

12. 18 U.S.C. § 3512(a), (d), (f) (current)

§ 3512. Foreign requests for assistance in criminal investigations and prosecutions

(a) Execution of request for assistance.—

(1) In general.—Upon application, duly authorized by an appropriate official of the Department of Justice, of an attorney for the Government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the

prosecution of criminal offenses, including proceedings regarding forfeiture, sentencing, and restitution.

(2) Scope of orders.—Any order issued by a Federal judge pursuant to paragraph (1) may include the issuance of—

***

(B) a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703 of this title;

***

(d) Search warrant limitation.—An application for execution of a request for a search warrant from a foreign authority under this section, other than an application for a warrant issued as provided under section 2703 of this title, shall be filed in the district in which the place or person to be searched is located. ….

***

(f) Service of order or warrant.—Except as provided under subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States.

***

13. Federal Rules of Criminal Procedure, Rule 41 (current)

Rule 41. Search and Seizure

(a) Scope and Definitions.

(1) Scope. This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.

(2) Definitions. The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.

(C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant.

(D) "Domestic terrorism" and "international terrorism" have the meanings set out in 18 U.S.C. § 2331.

(E) "Tracking device" has the meaning set out in 18 U.S.C. § 3117(b).

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside

the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

(c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following:

(1) evidence of a crime;

(2) contraband, fruits of crime, or other items illegally possessed;

(3) property designed for use, intended for use, or used in committing a crime; or

(4) a person to be arrested or a person who is unlawfully restrained.

(d) Obtaining a Warrant.

(1) In General. After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.

(2) Requesting a Warrant in the Presence of a Judge.

(A) Warrant on an Affidavit. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

(B) Warrant on Sworn Testimony. The judge

may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) Recording Testimony. Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) Requesting a Warrant by Telephonic or Other Reliable Electronic Means. In accordance with Rule 4.1, a magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means.

(e) Issuing the Warrant.

(1) In General. The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and

(iii) return the warrant to the magistrate judge designated in the warrant.

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(C) Warrant for a Tracking Device. A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:

(i) complete any installation authorized by the warrant within a specified time no longer than 10 days;

(ii) perform any installation authorized by

the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and

(iii) return the warrant to the judge designated in the warrant.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(A) Noting the Time. The officer executing the warrant must enter on it the exact date and time it was executed.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

(C) Receipt. The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or

from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

(D) Return. The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant. The officer may do so by reliable electronic means. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(2) Warrant for a Tracking Device.

(A) Noting the Time. The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used.

(B) Return. Within 10 days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant. The officer may do so by reliable electronic means.

(C) Service. Within 10 days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3).

(3) Delayed Notice. Upon the government's request, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—may delay any notice required by this rule if the delay is authorized by statute.

(g) Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

(h) Motion to Suppress. A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

(i) Forwarding Papers to the Clerk. The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.

14. Federal Rules of Criminal Procedure, Rule 41(a) (1986)

Rule 41. Search and Seizure

(a) AUTHORITY TO ISSUE WARRANT. A search warrant authorized by this rule may be issued by a federal magistrate or a judge of a state court of record within the district wherein the property or person sought is located, upon request of a federal law enforcement officer or an attorney for the government.

15. Commission Regulation 2016/679, 2016 O.J. (L 119) 64 (European Union "General Data Protection Regulation")

***

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international

agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to

providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

***