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 BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, ELECTRONIC FRONTIER FOUNDATION, RESTORE THE FOURTH, INC. AND R STREET INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

FAIZA PATEL
MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Sixth Avenue, 12th Floor
New York, NY 10012

Counsel for Brennan Center for Justice at NYU School of Law

BRETT J. WILLIAMSON
Counsel of Record
NATHANIEL ASHER
DAVID K. LUKMIRE
O'MELVENY & MYERS LLP
Times Square Tower
Seven Times Square
New York, NY 10036
(212) 326-2000
bwilliamson@omm.com

Counsel for Amici Curiae

(For Continuation of Appearances See Inside Cover)

277573

David D. Cole
American Civil Liberties
Union Foundation
915 15th Street, NW
Washington, D.C. 20005

Jennifer Stisa Granick
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111

Counsel for American Civil Liberties Union Foundation

Arthur Rizer
Charles Duan
R Street Institute
1212 New York Avenue NW,
Suite 900
Washington, DC 20005

Counsel for R Street Institute

Lee Tien
Andrew Crocker
Electronic Frontier
Foundation
815 Eddy Street
San Francisco, CA 94109

Counsel for Electronic Frontier Foundation

Mahesha P. Subbaraman
Subbaraman PLLC
222 South Ninth Street,
Suite 1600
Minneapolis, MN 55402

Counsel for Restore the Fourth, Inc.

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Page

Cited Authorities

Page

Page

CONSTITUTIONAL PROVISIONS, STATUTES AND RULES

Page

OTHER AUTHORITIES

Page

INTEREST OF *AMICI CURIAE*[1]

Amici the Brennan Center for Justice, the American Civil Liberties Union, the Electronic Frontier Foundation, Restore the Fourth, and the R Street Institute are organizations committed to ensuring that constitutional rights are protected as electronic communications technology continues to advance.

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous *amicus* briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211

1. The parties' letters consenting to the filing of all amicus briefs have been filed with the Clerk's office. Under Supreme Court Rule 37.6, counsel for *amici* state that no party's counsel authored any portion of this brief, that no party or party's counsel contributed money intended to fund this brief's preparation or submission, and that no persons other than the *amici*, their members, or their counsel contributed money that was intended to fund this brief's preparation or submission. This brief does not purport to represent the position of NYU School of Law.

(2017); *Riley v. California*, 134 S.Ct. 2473 (2014); *United States v. Jones*, 132 S.Ct. 945 (2012); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 569 (2016); *United States v. Moalin*, No. 13-50572 (9th Cir. filed Nov. 5 2015); and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

The American Civil Liberties Union is a nationwide, non-profit, non-partisan organization with approximately 1.6 million members dedicated to defending the principles embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has appeared before the federal courts on numerous occasions, both as direct counsel and as *amicus curiae*. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to the organization and its members.

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 44,000 dues-paying members that works to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has filed *amicus* briefs with this Court in numerous cases applying privacy law to emerging technology. *See, e.g.*, *Carpenter v. United States*, No. 16-402; *Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct. 1958 (2013); *United States v. Jones*, 565 U.S. 400 (2012); *City of Ontario v. Quon*, 560 U.S. 746 (2010). EFF is based in the United States. EFF is a member of European Digital Rights ("EDRi"), which is joining a different *amicus* brief in this case filed by Privacy International ("PI"); EFF does not join PI's brief.

Restore the Fourth, Inc. ("Restore the Fourth") is a national, non-partisan civil liberties organization dedicated to the robust enforcement of the Fourth Amendment. Restore the Fourth believes that everyone is entitled to privacy in their persons, homes, papers, and effects and that modern changes to technology, governance, and law should foster—not hinder—the protection of this right. Restore the Fourth advances these principles by overseeing a network of local chapters whose members include lawyers, academics, advocates, and ordinary citizens. Each chapter devises a variety of grassroots activities designed to bolster political recognition of Fourth Amendment rights. On the national level, Restore the Fourth also files *amicus curiae* briefs in significant Fourth Amendment cases.[2]

The R Street Institute is a non-profit, non-partisan public-policy research organization. R Street's mission is to engage in policy research and educational outreach that promotes free markets, as well as limited yet effective government, including properly calibrated legal and regulatory frameworks that support Internet economic growth and individual liberty. R Street's particular focus on Internet law and policy is one of offering research and analysis that show the advantages of a more market-oriented society and of more effective, more efficient laws and regulations that protect freedom of expression and privacy.

---

2. *See, e.g.*, Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Petitioner, *Collins v. Virginia*, No. 16-1027 (U.S. filed Nov. 17, 2017); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Petitioner, *Byrd v. United States*, No. 16-1371 (U.S. filed Nov. 16, 2017); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Petitioner, *Carpenter v. United States*, No. 16-402 (U.S. filed Aug. 14, 2017).

INTRODUCTION AND SUMMARY OF THE ARGUMENT

The government invites this Court to make three critical missteps, all of which could have far-reaching and unintended consequences for the future of digital privacy rights in the United States.

First, the government urges the Court to hold that the Fourth Amendment is not implicated when the government or its agents copy or transfer a user's emails, but only upon disclosure or review of the emails' content. To the contrary, if Microsoft copies, transfers, or otherwise accesses email at the government's behest, the Fourth Amendment applies and requires a warrant. This is because Microsoft is acting as a government agent and seizing the user's private communications on the government's behalf, even before an investigator reads them. Thus, a Fourth Amendment "search and seizure" occurs when Microsoft accesses, copies, or moves a user's data to fulfill the government's demand, regardless of when, where, or even whether investigators might later search it. Were this Court to suggest otherwise, the government could then try to compel companies to copy, transfer, decrypt, analyze, or give government agents log-on access to user email accounts to make private data searchable to investigators—all without obtaining a warrant or undergoing constitutional scrutiny. Prohibiting these kinds of seizures for the purpose of gathering private information is exactly why the founders adopted the Fourth Amendment in the first place.

Second, the government conflates subpoenas with search warrants, implying that the former are sufficient to

search and seize emails. Pet. Br. at 36 ("With a subpoena, a court 'may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates.'" (citing Fed. R. Crim. P. 17(c)(1))). In fact, a subpoena constitutionally *cannot* compel disclosure of a customer's email or other private communications under the Fourth Amendment. Emails, like text messages, are "essential means or necessary instruments for self-expression, even self-identification," *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). As a result, government access to them invades a reasonable expectation of privacy and generally requires a warrant based on probable cause. *See United States v. Warshak*, 631 F.3d 266, 285–86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."). In short, subpoenas are insufficient instruments for accessing email through a service provider under the Fourth Amendment. *Amici* urge the Court to make clear that a mere subpoena cannot authorize law enforcement to search and seize American email from a service provider.

Third, the government's position will increase the risk that investigative demands from other countries' governments will interfere with the privacy and property interests of people in the United States. If this Court holds that the U.S. government can compel disclosure of foreign data from any service provider with operations in the United States, then foreign governments are more likely to reciprocate by seeking Americans' data through service providers with a presence abroad. As a result, U.S. communications providers such as Microsoft will have less ability to contest foreign government demands to copy and

search communications belonging to U.S. persons, even though foreign legal standards may be far less protective than those applicable in this country.

Amici urge the Court to avoid these missteps, which could dramatically curtail Fourth Amendment rights for Americans' electronic communications data.

ARGUMENT

I. The moment of collection is a seizure regulated by the Fourth Amendment.

The Second Circuit correctly held that a customer's privacy is invaded at the time and place her emails are accessed or copied by a provider acting as a government agent, and not only when they are later disclosed to investigators. *See* Pet. App. 11a, 43a–44a & n.27 ("[T]he invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government."); *see also* Pet. App. 85a. The government resists this holding, maintaining that no invasion of privacy occurs until "Microsoft discloses information to the government and the government reviews that information." Pet. Br. 26. The government is wrong for at least two reasons. First, the Fourth Amendment's guarantee against unreasonable seizures extends to private parties acting as agents of the government. *See Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989) ("[T]he [Fourth] Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government."). Second, when a government agent copies, transfers, or otherwise accesses private

communications, it is a seizure governed by the Fourth Amendment and requires a warrant. *Cf. Arizona v. Hicks*, 480 U.S. 321, 325 (1987) (concluding that moving an object, "even a few inches" is "much more than trivial for purposes of the Fourth Amendment").

A. Stored Communication Act warrants conscript communications providers to act as government agents regulated by the Fourth Amendment.

Any action Microsoft takes to comply with a law enforcement demand for access to customer emails is government action subject to the Fourth Amendment. It is well-settled that a private party becomes an agent of the government when compelled to assist in conducting a search or seizure. *See Skinner*, 489 U.S. at 614; *United States v. Jacobsen,* 466 U.S. 109, 113 (1984). The test is whether the private party, "in light of all the circumstances," would be acting as an "instrument" or agent of the state. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971). Relevant factors include whether the government instigated the search, whether the private party's primary goal was to assist law enforcement, and the degree of government knowledge and acquiescence. *See United States v. Ackerman*, 831 F.3d 1292, 1301 (10th Cir. 2016) (Gorsuch, J.) (describing approaches taken by various circuit courts). Here, every factor points toward the conclusion that Microsoft would be acting as a government agent were it to take steps to comply with a Stored Communications Act (SCA) warrant: (1) the government instigated the search; (2) Microsoft would act only for the purpose of assisting law enforcement; and (3) the government is fully aware of the steps Microsoft would take to fulfill its demand. The SCA order would

thus conscript Microsoft to conduct a search and seizure on the government's behalf.

Even though Microsoft could independently access, copy, or move the emails when acting as a private party, the Fourth Amendment still applies if Microsoft takes these actions at the government's behest. The SCA expressly anticipates that law enforcement will require service providers to perform state functions in executing a warrant under Section 2703. *See* 18 U.S.C. § 2703(g) (stating that the presence of an officer "shall not be required" for service or execution of an SCA warrant). The government needs Microsoft's cooperation because government investigators do not have the ability to locate, access, and copy Microsoft users' data on their own. Indeed, when the government conscripts a private party to help execute a search or seizure, it commonly does so because the private party has both the physical and lawful ability to provide assistance. Contrary to the government's implication, private parties do not act as government agents only when they are breaking the law. A hotel owner has legal authority to enter a guest's room, but it is a search for her to do so at the police's behest. *See Stoner v. California*, 376 U.S. 483 (1964) (illegal search when hotel clerk let police into guest's room). An employee may enter his work premises and report wrongdoing he sees there, but that "furnishes no justification for federal agents to enter a place of business from which the public is restricted and to conduct their own warrantless search." *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 315 (1978). For the same reasons, the government is wrong to argue that because Microsoft has the legal ability to migrate accounts between the United States and Ireland, it is not a search or seizure for the company to do so at the government's demand.

To support its argument that communications providers are not government agents when copying or moving data to comply with an SCA warrant, the government cites *California Bankers Association v. Shultz*, 416 U.S. 21, 52–54 (1974), in which the Court held that a private bank's compliance with federal recordkeeping requirements did not transform the bank into a government agent. But that case says only that no seizure occurs when the government requires a bank to maintain business records of financial transactions *to which the bank is a party*, and in which neither the bank nor the customer has a reasonable expectation of privacy. *Id.* at 52. By contrast, individuals do have both a property interest and a privacy interest in their emails. As explained in Section II.B, *infra*, the compelled collection and disclosure of emails requires a warrant. If forced under court order to gather or transfer these materials for law enforcement, the company is acting as a government agent. For Fourth Amendment purposes, it is irrelevant that a Microsoft technician, and not an FBI agent, is responsible for actually clicking the buttons to copy or move personal communications. *See Jacobsen,* 466 U.S. at 113. Rather, as the Sixth Circuit determined in *United States v. Warshak*, "if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search." 631 F.3d 266, 286 (6th Cir. 2010). In sum, Microsoft would be acting as a government agent when copying and transferring a user's emails on the government's behalf, triggering a Fourth Amendment analysis.

B. Copying data infringes on the owner's possessory interests and is therefore a seizure.

Requiring a service provider to copy and/or transfer customer emails in response to a warrant is a Fourth Amendment seizure. When done for purposes of gathering private information, it is also a search. The government argues that Microsoft's collection and copying of email does not interfere with the user's possessory interests, Pet. Br. at 31, but ignores that a core element of property ownership is the right to exclude. Furthermore, the government's argument that such collection and copying does not "expand[ ] [Microsoft's] authority over those emails" (*id.*) ignores that it *does* expand the *government's* authority over them. A government-directed exercise of dominion over an individual's private communications is, by itself, a Fourth Amendment seizure.

A seizure occurs when "there is some meaningful interference with an individual's possessory interests in that property." *Jacobsen*, 466 U.S. at 113. "[O]ne of the most essential sticks in the bundle of rights that are commonly characterized as property" is "the right to exclude others." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). Copying or moving data is a seizure because it interferes with the user's possessory interests in controlling the flow of, and access to, her data. *See United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc) (referring to copying of electronic data as seizure throughout opinion); *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (same); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (describing information retrieval by Yahoo technicians from two e-mail accounts as a "seizure"); *In re*

A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.Com Maintained at Premises Controlled by Google, Inc., No. 14 Mag. 309, 2014 WL 3583529, at *4–5 (S.D.N.Y. Aug. 7, 2014) (copying of electronic evidence equates to an "exercise of dominion essentially amount[ing] to a 'seizure' even if the seizure takes place at the premises searched and is only temporary"); *United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (obtaining copies of emails from internet service provider "for subsequent searching" is a seizure); *United States v. Bowen*, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (copying of entire email account described as seizure).

These cases reflect the practical reality that the government can meaningfully interfere with a user's property rights in email even if the user still has access to copies of the messages. A "seizure" is not limited to an act that entirely deprives a person of the use of her property. Rather, a government act that deprives the owner of meaningful control over her property is also a "seizure."

Thus, even though email communications may not take a physical form, copying digital data interferes with the user's possessory right to exclude others and is a Fourth Amendment event. *See Ackerman*, 831 F.3d at 1308 ("Of course, the framers were concerned with the protection of physical rather than virtual correspondence. But a more obvious analogy from principle to new technology is hard to imagine and, indeed, many courts have already applied the common law's ancient trespass to chattels doctrine to electronic, not just written, communications."). This is true because the value of email, like an old-fashioned letter, lies in its private communicative content and the ability to

exclude others from it. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Nat'l L. & Pol'y 247, 279 (2016). If the digital Fourth Amendment is to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *Jones*, 565 U.S. at 406 (quoting *Kyllo v. United States*, 533 U.S. 27, 34) (2001)) (alteration in original), this Court should recognize that copying or otherwise exercising dominion over electronic communications is the digital equivalent of the "trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment," *Ackerman*, 831 F.3d at 1307. Such actions undermine the "inviolability" of the data and thus constitute Fourth Amendment seizures. *See Jones*, 565 U.S. at 419 n.2.

The government suggests that the email owner's right to exclude is not implicated because Microsoft "already has custody and control of the targeted communications and the legal ability to move them at will," citing a dissenting opinion from the Second Circuit's denial of rehearing *en banc*. Pet. Br. at 27. Microsoft's authorization to access and transfer the owner's data for legitimate business purposes does not create a blanket authorization for Microsoft to do with that data whatever it, or the government, pleases. "The SCA constrains a service provider's use of that 'possession,' recognizing the provider's role as an intermediary between the customer who created the content and third parties." Pet. App. 111a–112a n.5 (Carney, J., concurring in denial of rehearing *en banc*). In *Berger v. New York*, this Court recognized that electronic eavesdropping is tantamount to seizing conversations despite the fact that "[t]he telephone conversation itself must be electronically transmitted by telephone company

equipment, and may be recorded or overheard by the use of other company equipment." 388 U.S. 41, 59 (1967). Similarly, Microsoft is an intermediary in the electronic transmission of email, and government-ordered access to or manipulation of those messages is regulated by the Fourth Amendment.

Further, transferring data from Ireland to the United States is no small matter for Fourth Amendment purposes. In *Arizona v. Hicks*, the Court found that where a police officer had lawfully entered the respondent's apartment to search for a shooter, victims, and weapons, "taking action" to move a stereo a few inches in order to "expose[] to view" a concealed serial number was a separate invasion of privacy, unrelated to the lawful objective of the authorized intrusion into the apartment. 480 U.S. at 324–25 ("[M]oving it even a few inches is much more than trivial for purposes of the Fourth Amendment." (internal quotation marks omitted)). The government could not reasonably argue that a storage vendor's ability to move archived paper files from one warehouse to another means that there is no seizure when law enforcement orders such a transfer to facilitate a government search.

Ultimately, the government defines the right to exclude too narrowly. It overlooks the ways in which transferring and copying data for purposes of disclosing it to the government is an exercise of government dominion. The government demands that Microsoft take actions that would give the government control over the data that it did not have before and that the user did not authorize. For example, the government does not argue that Microsoft would be free to delete the account data instead of providing it to the government after

receiving the warrant. Instead, acting as an agent of the government, Microsoft must preserve, copy, and transfer email messages for the purpose of disclosing them to government investigators. Such actions are plainly not "primarily the result of private initiative," but bear "clear indices of the Government's encouragement, endorsement, and participation." *Skinner*, 489 U.S. at 615. Imposing an obligation on Microsoft to take these actions implicates the Fourth Amendment.

Because it would be done to gather information, the contemplated access, transfer, and manipulation of email messages by Microsoft would also constitute a Fourth Amendment "search." In *Jones*, the government attached a GPS tracking device to a car and used it to track the vehicle. The defendant retained full possession and use of the car. It was nevertheless a Fourth Amendment event when the government intruded on those property interests to gather information. *Id.* at 404–05. The Court explained that "[a] trespass on 'houses' or 'effects'"—*i.e.*, an infringement of the right to exclude others—is a search when carried out "to obtain information," regardless of whether any resulting interference is "meaningful." *See* 565 U.S. at 408 n.5; *see also Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (recognizing the right to exclude as a basis for privacy interests). And as Justice Alito noted, the common law previously permitted a chattel owner to pursue a trespass claim even absent damage to the chattel, so long as the "dignitary interest in the inviolability of chattel[]" was harmed. *See* 565 U.S. 400, 419 n.2 (internal quotation mark omitted); *see also Ackerman*, 831 F.3d at 1307–08 (recognizing that an individual's ability to exclude others from accessing data is akin to a property owner's right to prevent trespasses to her chattel). Similarly,

in *Hicks*, 480 U.S. at 325, the officer moving stereo components even a few inches to view serial numbers and determine whether the components were stolen was a search.

In sum, a "search and seizure" for Fourth Amendment purposes occurs as soon as Microsoft, acting as a government agent, copies or transfers a user's data for purposes of disclosing it to the government. *See Jacobsen,* 466 U.S. at 113, n.5 ("While the concept of a 'seizure' of property is not much discussed in our cases, this definition follows from our oft-repeated definition of the 'seizure' of a person within the meaning of the Fourth Amendment—meaningful interference, *however brief*, with an individual's freedom of movement." (emphasis added)). Because the government's exercise of control over the user's data meaningfully interferes with her right to exclude others, the data is seized the moment it is copied at the government's command. And because the invasion of property is for purposes of gathering information, the emails are also subject to a "search" when the government compels Microsoft to access, copy, or transfer them to facilitate government collection of information. From either perspective, the Fourth Amendment is triggered at the moment Microsoft accesses or copies the emails or causes them to be transferred from abroad.

C. The government's position that the search and seizure occur only when data is examined has dangerous practical consequences.

Adopting the government's position that a seizure does not occur until investigators actually receive and examine the emails is not just inconsistent with existing

law; it contradicts the fundamental purposes of the Fourth Amendment. It also could have far-reaching negative consequences.

The Framers enacted the Fourth Amendment to protect individuals from unreasonable government searches and seizures, including the infamous "general warrants" that gave customs officers blanket authority to search and seize private houses, papers, and effects. *See Marron v. United States*, 275 U.S. 192, 195–96 (1927). Consequently, the *Berger* Court condemned wiretaps that fail to particularly describe the "property" to be intercepted because they give law enforcement "a roving commission to 'seize' any and all conversations." *Berger*, 388 U.S. at 58–59 (1967). And in *Stanford v. Texas*, the Court added that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain." 379 U.S. 476, 511–12 (1965). Yet the government seeks a rule that would permit the wholesale copying of a user's email account for purposes of disclosing it to government investigators, *without* triggering the Fourth Amendment's warrant requirement. Accepting the government's argument could lead to massive over-collection of data. On this theory, a warrant would not be required to copy *all* electronic communications, unless and until officers sought to view some of the data. The government's view would usher in the modern equivalent of a general warrant, like "fetch[ing] a sack, and fill[ing] it" with all of a person's private papers. *See Wilkes v. Wood*, Lofft 1, 4, 98 Eng. Rep. 489, 491 (C.P. 1763).

The government's demand implicates privacy and property interests in our most personal information. JA 25. With the advent of "cloud computing," a user's email account not only contains individual messages and their subject lines, but may also contain vast archives of personal information, including private photographs, medical records, and other personal files uploaded for storage. *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014). Much like modern cell phones, *see id.* at 2490, the data associated with a user's Microsoft account is qualitatively different from caches of physical records, as it could include a host of sensitive and revealing records generated by a suite of functions and "apps" in addition to email.[3] If there is no Fourth Amendment intrusion until a human being actually examines copied data, the government could collect data belonging to anyone, without a warrant or any individualized suspicion, just in case it might be useful at some later point. The Court should reject this possibility and uphold crucial Fourth Amendment protections against government overreach.

II. Subpoenas are not sufficient to compel disclosure of emails stored abroad.

The Court should reject the government's argument that Congress intended both subpoenas and warrants under the SCA to compel extraterritorial searches and seizures of private communications. The government

3. *See, e.g.,* https://products.office.com/en-us/exploreoffice-for-home (offering use of Microsoft Word, Excel, PowerPoint, Outlook, OneNote, Publisher and Access, as well as one terabyte of cloud file storage and integration with Skype, an audio/video/messaging service used to interact with mobile phones and landlines.)

posits that SCA warrants must have extraterritorial reach because (i) Congress passed the SCA against a "backdrop" of the extraterritorial reach of subpoenas and (ii) SCA warrants are executed like subpoenas. Pet. Br. at 32–41. But the pre-1986 cases allowing the use of subpoenas to obtain foreign-stored business records arose in a materially different context, and they do not establish that Congress intended the SCA to have the reach that the government advocates here. These cases involve corporate business records, not private messages and personal data transmitted by communications service providers. Congress could not have envisioned the massive transformation in email usage that has taken place since 1986, including third-party service providers' use of warehouses of servers all over the world. Thus, Congress's understanding of the reach of business-record subpoenas in 1986 does not determine how the government may obtain modern-day emails.

None of the cases the government relies on as evidence of congressional understanding and intent involve emails held by a service provider. Instead, those cases permitted the government to use subpoenas to obtain the following materials stored abroad:

- corporate records "pertaining to the operations of eight foreign companies," *In re Sealed Case*, 832 F.2d 1268, 1270, 1271 (D.C. Cir. 1987), abrogated on other grounds by *Braswell v. United States*, 487 U.S. 99 (1988);

- "financial documents," such as "[c]ertificates of [d]eposits, checking account statements, and deposit slips," *United States v. Bank of Nova Scotia*, 740 F.2d 817, 819–22 (11th Cir. 1984);

- "business records relating to crude oil transactions," *Marc Rich & Co. v. United States*, 707 F.2d 663, 665 (2d Cir. 1983);

- a bank's documents "relating to any transaction" between two specified parties, *United States v. First Nat'l City Bank*, 396 F.2d 897, 898 (2d Cir. 1968); and

- "corporate books and records," including "certain stock certificates" and advertising literature," *Secs. & Exchange Comm'n v. Minas de Artesima*, 150 F.2d 215, 218 (9th Cir. 1945).

Notably, those cases all precede the explosion of email usage and cloud storage that occurred over the last twenty-five years. Well before the SCA's enactment, this Court acknowledged that using subpoenas to obtain, for example, a personal diary may present "[s]pecial problems of privacy." *Fisher v. United States*, 425 U.S. 391, 401 n.7 (1976). The Court also suggested that the analysis may differ where "First Amendment values" are implicated. *See id.* The compelled disclosure of an entire email account raises those very concerns. In contrast to these business records, emails are "the technological scion of tangible mail." *Warshak*, 631 F.3d at 286. They are more than that, too. Emails may be used to send oneself a reminder about a doctor's appointment, an internet link to parenting advice, or notes on a late-night flash of inspiration. Other emails may reflect everything from a user's reading habits (a running list of books to read, saved links to articles) to their eating habits (receipts from delivery services, restaurant reservation details). Emails thus can provide "a revealing montage of the user's life," all in a single location. *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

Amici urge the Court to make clear that a subpoena is *not* constitutionally sufficient to compel a service provider to disclose emails stored on behalf of a user—no matter where the emails are stored. *See Warshak*, 631 F.3d at 288. To the extent the SCA authorizes the use of subpoenas to obtain emails, it is unconstitutional.[4] Yet the government's argument suggests that a subpoena is sufficient to obtain any records in a party's control, including the entire contents of an email account. *See* Pet. Br. at 40 ("[I]f the government were to forgo a subpoena and instead obtain a Section 2703 warrant—under the higher showing of probable cause—it would lose its ability to demand certain foreign-stored emails."). In contrast, this Court has indicated that emails stored by service providers are protected by the Fourth Amendment's warrant requirement. In *Riley*, for example, the Court pointed to the widespread use of cloud-based services as a factor *increasing* the privacy concerns implicated by cell phone searches. *See* 134 S. Ct. at 2491. The Court has further indicated that the "third-party doctrine"—the assertion that one may lack a reasonable expectation of privacy in information knowingly and voluntarily revealed to "third parties"—is not absolute, *see Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (finding that hospital patient has reasonable expectation of privacy that test results will not be shared with nonmedical personnel

4. Notably, since 2013, the Department of Justice has adopted a policy "always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process." Pet. App. at 50a n.1 (citing H.R. Rep. No. 114-528, at 9 (2016)). *See also Warshak*, 631 F.3d at 288 ("To the extent that the SCA purports to permit the government to obtain [emails stored with a commercial ISP] warrantlessly, the SCA is unconstitutional.").

without consent), and that it is particularly "ill suited to the digital age," *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

Indeed, during oral argument in *Carpenter v. United States* earlier this term the government itself appeared to concede that searches and seizures of email require a warrant. There, the government acknowledged that communication contents, including emails, are not a service provider's business records and that the provider's "incidental access" to user communications "doesn't vitiate Fourth Amendment protection."[5] Tr. of Oral Argument, *Carpenter v. United States*, No. 16-402, at 45:3–46:7 (Nov. 29, 2017). For these reasons, the Court should take care not to adopt the government's analogy between extraterritorial subpoenas for business records and warrants for disclosure of email.

Email has become thoroughly ingrained as an essential means of private communication in modern life, and individuals have no practical choice but to entrust their intimate data to third parties such as Microsoft. The Court should make clear that these practical realities do not diminish longstanding Fourth Amendment protections in our private communications. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1877) ("Whilst in the mail, [letters] can

5. However, *Amici* urge the Court not to adopt the government's distinction between "content" and "non-content" information, such as metadata or routing information, which should also receive Fourth Amendment protection due to the highly sensitive personal information it can convey. *See Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015) (discussing "the startling amount of detailed information metadata can reveal").

only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").

III. Accepting the government's extraterritoriality arguments would threaten the privacy of people in the United States.

Accepting the government's position that it may compel disclosure of any data from any service provider with operations in the United States would threaten the privacy interests of people residing in the United States. A decision upholding the lawfulness of that approach could embolden foreign governments to demand data belonging to U.S. persons under standards far less protective than those applicable in this country. At the same time, that holding would severely undermine U.S. service providers' efforts to resist such demands.

The Government dismisses these practical reciprocity concerns as unrealistic, but this would not be the first time that United States policies on privacy and data collection had international influence. A similar "race to the bottom" effect arose after the 2013 revelations about the N.S.A.'s PRISM program and other U.S. intelligence-gathering activities. The most visible international reactions to the disclosures were outrage and calls for increased data privacy protections, but in at least some cases, other countries seem to have been inspired to ramp up their own surveillance efforts. Technology executives, including Facebook's chief security officer, have revealed that demands from foreign governments for access to user data "surge[d]" after

the extent of the access enjoyed by the N.S.A. came to light. *See* David E. Sanger & Nicole Perlroth, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. Times (June 6, 2014), https://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html. Vodafone even noted that "a 'small number' of governments around the world ha[d] demanded the ability to tap directly into its communication networks." *See id.*

Privacy advocates echoed these accounts of increased surveillance by foreign governments. A June 2015 report published by Privacy International and Amnesty International, for instance, stated that the organizations had observed more countries across the globe pursuing expanded surveillance of communications data, citing Pakistan, France, Switzerland, the Netherlands, and Egypt as examples. *See Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance* 14–15, 18, Privacy Int'l & Amnesty Int'l (June 2015).[6] Indeed, leaked documents revealing Egypt's efforts to establish a program for mass social media surveillance show that the country specifically sought a system that "has previously been used by the USA or European States." *Egypt's Plan for Mass Surveillance of Social Media an Attack on Internet Privacy and Freedom of Expression*, Amnesty Int'l (June 4, 2014).[7]

---

6. *Available at* https://www.amnestyusa.org/wp-content/uploads/2017/04/ai-pi_two_years_on_from_snowden_final_final_clean.pdf.

7. *Available at* https://www.amnesty.org/en/latest/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/.

The Government's emphasis on the fact that other countries already make unilateral demands for foreign-stored data, Pet. Br. at 46–47, overlooks the important gatekeeping role that service providers play. Microsoft does not dispute that it receives such requests from foreign governments—but it is well documented that Microsoft and other major U.S. service providers frequently refuse those requests as lacking legal authority. Yahoo, for instance, reports rejecting 2,960 of the 7,027 data requests it received from governments other than the United States in the second half of 2016. *Transparency Report - Government Data Requests: July through December 2016*, Yahoo, at 1–2, https://s.yimg.com/ge/toc/con/v1/Yahoo-TR__Govt-Data-Requests__July-Dec-2016-revised-v2.pdf (last visited Jan. 16, 2018). Yahoo explains that this category includes rejections based on jurisdictional defects:

> Yahoo may have possessed data responsive to the Government Data Request, but none was produced because of a defect or other problem with the Government Data Request (e.g., the government agency sought information outside its jurisdiction or the request only sought data that could not be lawfully obtained with the legal process provided). This category also includes Government Data Requests that were withdrawn after being received by Yahoo.

Id. at 4. *See also Report on Government and Private Party Requests for Customer Information*, Apple, 1 (2017), https://images.apple.com/legal/privacy/transparency/requests-2017-H1-en.pdf ("International requests for content stored in our data centers in the U.S. must comply with the U.S. Electronic Communications Privacy Act

(ECPA)."); *About Our Practices and Your Data*, Microsoft Data Law Blog, https://blogs.microsoft.com/datalaw/our-practices/#how-does-microsoft-determine-countries-request-data (last visited Jan. 16, 2018) ("Microsoft produces data in response to valid legal requests from governmental entities in countries where we host the requested data."); Sanger & Perlroth, *supra*.

It is hardly realistic to expect that holding that SCA warrants have extraterritorial reach will result in *fewer* data requests from foreign governments. This Court's ruling should not give governments that have agreed to mutual legal assistance treaties with the United States an argument to side-step those obligations. The risk is that our MLAT partners will have little incentive to rely on those treaties when the United States itself is avoiding them and denouncing them as overly cumbersome. Indeed, a November 2014 report from the British Parliament's Intelligence and Security Committee identified U.S. service providers' refusal to honor U.K. interception warrants as a significant source of frustration. *See* Intel. & Sec. Comm. of Parliament, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* 141–42, 149, 151 (Nov. 25, 2014).[8] A holding that a government can compel service providers operating within their borders to disclose any data they can access could provide foreign governments with just the "lever to compel assistance" that the Committee sought. *See id.* at 141. This result would expose millions of Americans who do business with globally operated service providers to potential foreign surveillance—and would leave the U.S. government without a leg to stand on to complain.

8. *Available at* https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20141125_ISC_Woolwich_Report%28website%29.pdf.

Apart from the specific statutory question presented, the Court should take care not to undermine service providers' ability to resist requests for data belonging to United States persons, especially when those requests do not meet our legal requirements and may offend our constitutional principles.

CONCLUSION

Amici urge the Court to avoid three missteps that could dramatically curtail Fourth Amendment rights for Americans' electronic communications data. Specifically, this Court should make clear both that when a provider collects or transfers information at government request, that conduct is regulated by the Fourth Amendment and that subpoenas are not sufficient to constitutionally compel disclosure of emails. Finally, the Court should not embolden foreign governments to demand data belonging to U.S. persons under standards far less protective of personal privacy than those applicable in this country.

Respectfully submitted,

Faiza Patel
Michael W. Price
Brennan Center for Justice
at NYU School of Law
161 Sixth Avenue, 12th Floor
New York, NY 10012

Counsel for Brennan Center for Justice at NYU School of Law

Brett J. Williamson
Counsel of Record
Nathaniel Asher
David K. Lukmire
O'Melveny & Myers LLP
Times Square Tower
Seven Times Square
New York, NY 10036
(212) 326-2000
bwilliamson@omm.com

Counsel for Amici Curiae

David D. Cole
American Civil Liberties
Union Foundation
915 15th Street, NW
Washington, D.C. 20005

Jennifer Stisa Granick
American Civil Liberties
Union Foundation
39 Drumm Street
San Francisco, CA 94111

Counsel for American Civil Liberties Union Foundation

Arthur Rizer
Charles Duan
R Street Institute
1212 New York Avenue NW,
Suite 900
Washington, DC 20005

Counsel for R Street Institute

Lee Tien
Andrew Crocker
Electronic Frontier
Foundation
815 Eddy Street
San Francisco, CA 94109

Counsel for Electronic Frontier Foundation

Mahesha P. Subbaraman
Subbaraman PLLC
222 South Ninth Street,
Suite 1600
Minneapolis, MN 55402

Counsel for Restore the Fourth, Inc.