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 OF *AMICI CURIAE* FOURTH AMENDMENT SCHOLARS IN SUPPORT OF THE RESPONDENT

MICHAEL VATIS
Counsel of Record
JEFFREY A. NOVACK
JOHANNA DENNEHY
MARCUS A. GADSON
STEPTOE & JOHNSON LLP
1114 Avenue of the Americas
New York, New York 10036
(212) 506-3900
mvatis@steptoe.com

Counsel for Amici Curiae

278115

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

Cases

Cited Authorities

Page

Cited Authorities

Page

Statutes

Rules

Law Review Articles

Cited Authorities

Page

INTEREST OF AMICI CURIAE[1]

The amici curiae—whose biographies appear in the appendix—are constitutional scholars who have studied the Fourth Amendment and its history. They have an interest in seeing that the Electronic Communications Privacy Act (of which the Stored Communications Act is a part) is interpreted consistently with the Founders' understanding that property rights undergird the Fourth Amendment.

SUMMARY OF ARGUMENT

Although this case involves technologies developed relatively recently, the issue it presents can be resolved by drawing on principles of property law that are embedded in the text of the Fourth Amendment and that have animated its interpretation since its ratification in 1791. Because execution of the warrant at issue in this case would require a trespass upon an email user's property (as well as an invasion of his privacy) in Ireland, such execution would result in an impermissible extraterritorial application of the Stored Communications Act ("SCA").

---

1. Pursuant to Supreme Court Rule 37.6, the amici curiae affirm that no counsel for a party authored this brief in whole or in part; that no party or counsel for a party made a monetary contribution toward the preparation or submission of this brief; and that no person other than the amici curiae or their counsels made a monetary contribution to its preparation or submission. Pursuant to Supreme Court Rule 37.3, each party has consented to the filing of this brief, and copies of the consents are on file with the Clerk of the Court.

Accordingly, the judgment below should be affirmed.

ARGUMENT

A constitutionally significant event occurs when property is seized or searched, whether by direct physical intrusion or by the use of technology from a remote location. This intrusion occurs at the location of the property, regardless of the location from which the Government conducts the seizure or search, and regardless of whether the Government conducts the action itself or through an agent. Execution of the warrant at issue here would intrude upon property because the emails sought by the government here are the property of the Microsoft email user, and that intrusion would occur in Ireland, the locus of the emails. Compelling Microsoft to access and copy emails stored on a server in Ireland therefore would constitute an impermissible extraterritorial application of the SCA, even if the ultimate disclosure of information to the Government occurred in the United States.

I. Property Rights Lie at the Core of the Fourth Amendment.

Protecting citizens' property rights was "the 'great focus'" of the Founders. Steven J. Eagle, *The Development of Property Rights in America and the Property Rights Movement*, 1 Geo. J.L. & Pub. Pol'y 77, 83 (2002). Just seven years after the Constitution's ratification, Justice Patterson declared "that the right of acquiring and possessing property, and having it protected, is one of the natural, inherent, and unalienable rights of man" and that "[t]he preservation of property then is a primary object of the social compact." *Van Horne's Lessee v. Dorrance*, 2 U.S. (2 Dall.) 304, 310 (1795).

This core right was enshrined in the Fourth Amendment. In 1886, the Court recognized in *Boyd v. United States* that the Fourth Amendment was "framed" to fit the fact that "[t]he great end for which men entered into society was to secure their property." 116 U.S. 616, 627 (1886) (quoting *Entick v. Carrington*, (1765) 95 Eng. Rep. 807; 19 How. St. Tr. 1029, 1066). Because Fourth Amendment rights are defined in terms of our "persons, houses, papers, and effects," until recent decades, this Court employed property-based rules to determine whether there was a search or seizure within the meaning of the Fourth Amendment. *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 405 (2012) (confirming that "our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century"). Under this approach, an intrusion into or upon an individual's property was the archetypal Fourth Amendment search or seizure. *Id.*

In 1967, this Court supplemented its property-based approach by recognizing that, in addition to protecting individuals against trespass to their property, the Fourth Amendment guarantees a reasonable expectation of privacy. *See Katz v. United States*, 389 U.S. 347 (1967); *see also Jones*, 565 U.S. at 409 (recognizing that the reasonable expectation of privacy test "has been added to, not substituted for, the common-law trespassory test").

Today, a majority of the Justices of this Court have recognized that these two approaches complement one another. Indeed, they often lead to the same result, because traditional property-based rights inform the reasonable expectation of privacy test. In 2012, Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor joined

Justice Scalia's majority opinion in *United States v. Jones*, which affirmed that the reasonable expectation of privacy test is based in part on "concepts of real or personal property law." *Id.* at 407–08 (quoting *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)). In 2013, Justices Kagan, Ginsburg, and Sotomayor similarly identified the linkage and overlap between the right against trespass on property and the right to a reasonable expectation of privacy. *See Florida v. Jardines*, 569 U.S. 1, 13 (2013) (Kagan, J., concurring). They observed that the two rights may align in scope because "[t]he law of property 'naturally enough influence[s]' our 'shared social expectations' of what places should be free from governmental incursions." *Id.* (quoting *Georgia v. Randolph*, 547 U.S. 103, 111 (2006)).

II. A Constitutionally Significant Intrusion Occurs at the Location of the Property, Regardless of the Place from Which the Government Conducts the Search or Seizure or the Means It Uses.

This Court has long understood that a constitutionally significant intrusion occurs where property is located when it is searched or seized, regardless of the location from which the government conducts the search or seizure or the means by which it does so. For example, the Court concluded in 1961, in *Silverman v. United States*, that police violated the Fourth Amendment when they touched a heating duct serving the defendants' home with a "spike mike," which allowed them to overhear the defendants' conversations from their observation post in an adjacent house. 365 U.S. 505 (1961).[2] The Court

2. The "spike mike" was a microphone attached to a foot-long spike, "together with an amplifier, a power pack, and earphones."

found that the placement of the spike mike violated the Fourth Amendment because it effected "an unauthorized physical penetration into the premises occupied by the [defendants]." *Id.* at 509. Even though the police themselves were not on the defendants' premises, and the spike mike only "touched" the defendants' heating duct, *id.*, the crucial fact to the Court was that the "officers overheard the [defendants'] conversations only by usurping part of the [defendants'] house or office," *id.* at 511.

The Court's recent decisions have reaffirmed that a Fourth Amendment search or seizure can occur when the Government gathers information from a place removed from the target property's location, and even when the Government does not commit a physical trespass but engages in conduct that amounts to the equivalent of a trespass.

In *Kyllo v. United States*, for instance, the Court concluded that the Government's use of a "thermal-imaging device" to "detect relative amounts of heat within the home" was a search of the home notwithstanding the fact that the search was conducted "from a public street." 533 U.S. 27, 29 (2001). This data collection from a remote location was a Fourth Amendment intrusion because it revealed information about details of the defendant's

---

Silverman, 365 U.S. at 506. The police inserted the spike under a baseboard in a room of a vacant house adjoining the defendants' premises and into a crevice in the "party wall" separating the two properties, where the spike made contact with a heating duct serving the defendants' premises, "thus converting [defendants'] entire heating system into a conductor of sound" and making the defendants' conversations "audible to the officers through the earphones." *Id.* at 506–07.

home that could not otherwise have been obtained without physical trespass onto the property. *Id.* at 40.

Other recent decisions have involved physical trespasses upon private property. In *United States v. Jones,* this Court held that federal agents committed an unconstitutional trespass by attaching a GPS monitoring device to a person's vehicle, and using that device to send data to a government computer at a remote location. 565 U.S. at 403–04. The Court found that by attaching the GPS device, the government had "physically occupied private property for the purpose of obtaining information." *Id.* at 404. It had "no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted," *id.* at 404–05 (citation omitted), even though the physical intrusion was arguably trivial and the information the device gathered was not disclosed to the Government until it was electronically "relayed" to a remote "Government computer," *id.* at 403.

In *Florida v. Jardines*, the Court concluded that the use of a trained police dog to detect odors emanating from within a home was part of an unlawful search, notwithstanding the fact that police officers have a general right to approach the home by entering the curtilage. 569 U.S. 1, 8 (2013). The Court found it significant that the "officers learned what they learned [about the interior of the home] only by physically intruding on Jardines' property to gather evidence" and concluded that this was "enough to establish that a search occurred." *Id.* at 11. The property-based rationale for finding a Fourth Amendment violation was so clear that the majority found no need to "decide whether the officers' investigation of Jardines' home violated his expectation of privacy under *Katz*." *Id.*

III. The Emails at Issue Here Are the Property of the Email User.

Courts have long recognized that forms of communication such as letters are the property of the parties to the communication, who enjoy an expectation of privacy in their contents even after the communications are sent via the postal service or another third party. This Court has confirmed that principle in a variety of settings, beginning with one of its early decisions interpreting the Fourth Amendment. *See Ex parte Jackson*, 96 U.S. 727, 732–33 (1877) (holding that letters and packages cannot be opened and inspected while in transit via the U.S. Postal Service, because "[l]etters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles"); *see also United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."). In addition, in the years following ratification of the Constitution, courts recognized that the contents of private letters are the property of the author under common law rules. *See, e.g., Woolsey v. Judd*, 11 How. Pr. 49, 55 (N.Y. Super. Ct. 1855) ("[T]he publication of private letters, without the consent of the writer, is an invasion of an exclusive right of property, which remains in the writer, even when the letters have been sent to, and are still in the possession of his correspondent."); *see also* Morgan Cloud, *Property is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 Am. Crim. L. Rev. 37, 56–58 (2017).

This same principle applies to other forms of private communication. Among the earliest Justices to recognize this were two dissenters in *Olmstead v. United States*—Justice Butler and Justice Brandeis. Justice Butler wrote that telephone communications "belong to the parties between whom they pass," not the party that delivers or stores the communications. *Olmstead v. United States*, 277 U.S. 438, 487 (1928) (Butler, J., dissenting). Similarly, Justice Brandeis observed that there is, "in essence, no difference between the sealed letter and the private telephone message." *Id.* at 475 (Brandeis, J., dissenting). Nearly four decades later, a majority of this Court agreed that oral communications that were recorded using a "bugging" device placed in a suspect's office were a form of "property" that required a particularized warrant. *Berger v. New York*, 388 U.S. 41, 58–59 (1967).

Lower courts and commentators have reached similar conclusions with respect to newer forms of communication, including emails. *See, e.g.*, *United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016) (Gorsuch, J.) ("No one in this appeal disputes that an email is a 'paper' or 'effect' for *Fourth Amendment* purposes, a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more."); *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (recognizing that digital information is equivalent to "personal 'papers'"); *LeClair v. Hart*, 800 F.2d 692, 696 n.5 (7th Cir. 1986) (recognizing that information is a form of property); *see also* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805 (2016) (arguing for an expansion of the understanding of Fourth Amendment "effects" to include "smart objects"

and the communications that emanate from them); Lon A. Berk, *After* Jones*, The Deluge: The Fourth Amendment's Treatment of Information, Big Data, and the Cloud*, 14 J. H. Tech. L. 1, 36 (2014) ("[I]t seems appropriate to conclude that data is property protected by the Fourth Amendment.").

Extending the Fourth Amendment framework to electronic communications and digital information is consistent with common sense. This Court has recognized that a person's electronic communications transmit and store sensitive information that the person would have transmitted and stored on paper in previous eras. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2491 (2014) ("A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

Treating email communications stored with a service provider as the property of the email user is fully consistent with the "third-party doctrine." That doctrine, as enunciated by this Court in *Smith v. Maryland* and *United States v. Miller*, holds that a person can lose privacy interests in some information disclosed to a third party. The leading cases, however, established this doctrine for information that was not the property of the individual defendant, but was the property of the third party and was created to permit the third party to perform its duties. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 741 (1979) ("Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a

'constitutionally protected area.'"); *id.* at 741–42 (noting that "pen registers do not acquire the *contents* of communications" but only dialing information, which is used by phone companies to complete calls, keep billing records, detect fraud, and prevent violations of law); *United States v. Miller*, 425 U.S. 435, 440 (1976) ("[T]he documents subpoenaed here are not respondent's 'private papers.' Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks."). In contrast, the content of emails remains the property of the email user, even when the emails are transmitted or stored by another entity. The email user does not lose his property-based privacy interest in the content of those emails, including rights against the trespass that a government seizure or search necessarily entails. Indeed, in *Riley*, this Court unanimously rejected the Government's argument that the Fourth Amendment permitted law enforcement to use a suspect's cell phone to access data stored remotely in the "cloud," reasoning that this "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." 134 S. Ct. at 2491. The "third-party doctrine" is, therefore, simply not relevant to the property rights at stake here.[3]

The emails at issue here are thus the property of the individual email account holder; they are not Microsoft's property. That legal conclusion is bolstered

3. For similar reasons, the Government's reliance (Gov't Br. at 14) on the *Bank of Nova Scotia* doctrine and cases like *Matter of Marc Rich & Co., A.G.*, 707 F.2d 663 (2d Cir. 1983), is misplaced. Those cases and their progeny involve subpoenas for a company's own records, not for property belonging to another party. *See Marc Rich*, 707 F.2d at 667.

by the contractual agreement between the individual account holder and Microsoft. Microsoft's Services Agreement specifically addressed the ownership of email communications. It states: "Who owns my Content that I put on the Services?" "You do." Reply Brief of Microsoft Corporation at 27, *Microsoft Corporation v. United States*, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985). Accordingly, while the Government and Microsoft are the parties to this dispute, it is an individual email account holder's property and privacy interests that are at stake.

IV. Emails Are Physically Encoded into the Storage Medium, and Have a Physical Presence in the Place Where They Are Stored.

Despite popular references to "the cloud" and "cyberspace," the reality is that emails and other electronic communications have a physical existence. These communications are not just theoretical constructs floating in the ether; though transmitted and stored in electronic media rather than on paper, they exist in physical manifestations, and those manifestations have physical loci. *See* Roderick O'Dorisio, *"You've Got Mail!" Decoding the Bits and Bytes of Fourth Amendment Computer Searches After* Ackerman, 94 Denv. L. Rev. 651, 671 (2017) (recognizing that electronic data is physically encoded onto hard drives).[4]

4. *See also United States v. Powers*, 2010 U.S. Dist. LEXIS 34007, at *5 (D. Neb. Mar. 4, 2010) ("E-mail accounts physically store e-mail messages and attachments on servers."); *In re United States*, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009) ("All materials stored online, whether they are e-mails or remotely stored documents, are physically stored on servers owned by an ISP.").

This Court recognized this reality in *Yates* v. *United States*, 135 S. Ct. 1074 (2015). There, a plurality of the Court observed that the term "tangible object" in 18 U.S.C. § 1519 includes data stored on an electronic storage medium. *Id.* at 1086. And, concurring in the judgment, Justice Alito specifically recognized that an "e-mail" is a "tangible object." *Id.* at 1089.

V. Execution of the Warrant Here Would Constitute an Impermissible Extraterritorial Application of the Stored Communications Act Since It Would Intrude on Property in Ireland.

Because the emails sought by the Government here are the property of the email user and those emails are physically located in Ireland, enforcement of the warrant in this case would necessarily constitute an impermissible extraterritorial application of the SCA. The Government's position to the contrary suffers from two fatal defects.

First, the Government contends that this case implicates only "abstract" privacy concerns with "no obvious territorial locus" because privacy is merely "a value or state of mind" which "lacks location." (Gov't Br. at 26–27 (quoting Judge Lynch, concurring in the judgement below, and Judge Jacobs, dissenting in the judgement below)). But, as demonstrated above, an email stored on a server is private property that has a physical existence and is stored in a physical location.

Second, by relying so heavily on jurisprudence involving subpoenas for the business records of the subpoenaed entity, and in arguing that a warrant issued under the SCA is not a warrant at all but actually a

subpoena, the Government is essentially contending that the emails at issue are the property of Microsoft, not the email user. (Govt. Br. at 29–30, 32–39). That is because subpoenas have traditionally only been used to obtain the *business records* of the subpoenaed entity, not property belonging to another person.[5] But the Government's position flies in the face of the long-standing jurisprudence recognizing that private communications, including emails, are the property of the parties to the communications, and that any seizure or search of those communications by the Government or an agent acting at

5. The Government suggests that subpoenas may be used to force a caretaker to turn over property belonging to another person, rather than a search warrant. *See* Gov't Br. at 40. But it cites only one district court case that has ever so held, *United States v. Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985). And even there, the court reasoned that the seizure of property did not violate the Fourth Amendment because the caretaker had voluntarily complied with the subpoena. *See id.* at 119. The other two cases cited by the Government do not bear the load the Government places on them. In *In re Grand Jury Subpoena Served Upon Horowitz*, the Second Circuit did not address the question, instead focusing on issues of overbreadth, attorney-client privilege, and the Fifth Amendment privilege against self-incrimination. *See* 482 F.2d 72, 75-83 (2d Cir. 1973). And this Court's decision in *Fisher v. United States* is totally inapposite. There, this Court held that compelled production from an attorney of records created by taxpayers' accountants did not implicate the taxpayers' Fifth Amendment rights. The case did not require the attorneys to turn over property of the taxpayer himself. *See* 425 U.S. 391, 414 (1976) ("Whether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his 'private papers.'") (citation omitted); *see also* Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805, 810–21 (2005) (contrasting subpoenas for business and private papers).

the command of the Government necessarily implicates the Fourth Amendment. For this reason, the email user's property-based privacy interest is infringed not only when and where the property is disclosed to, or examined by, the Government. That interest is also infringed when someone, acting under Government compulsion or on Government authority, seizes or searches the property. The infringement occurs where the property is located at the time of the seizure or search. In this case, that location is Ireland, for that is where Microsoft, acting on the Government's command, would search for the emails on its servers and seize them for transmittal to the Government.

CONCLUSION

The Government makes this case appear to be more complicated than it really is. It dissects the SCA and contends that each of its closely interrelated provisions actually has a different focus, and that the only relevant focus for this case is on "disclosure." It similarly dissects the execution of a warrant and contends that the only relevant action is the final step—the disclosure of the communications to the Government in the United States, not the actual searching for or seizing of them in Ireland.

But this case in fact is quite simple when viewed from the perspective of the Court's property-rights jurisprudence. *See Florida v. Jardines*, 569 U.S. at 11 ("One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy."). Because the emails sought by the Government are the property of the email account holder, and those emails are physically located in Ireland, any action by Microsoft to find

and retrieve those emails for the Government would necessarily result in a trespass on property in Ireland. Execution of the warrant would therefore constitute an impermissible extraterritorial application of the SCA.

Accordingly, the Court should affirm the judgment of the Second Circuit.

Respectfully Submitted,

Michael Vatis
Counsel of Record
Jeffrey A. Novack
Johanna Dennehy
Marcus A. Gadson
Steptoe & Johnson LLP
1114 Avenue of the Americas
New York, New York 10036
(212) 506-3900
mvatis@steptoe.com

Counsel for Amici Curiae

APPENDIX

APPENDIX — LIST OF *AMICI*

N.B. Institutional affiliations are for identification purposes only.

Valena Beety is a Professor of Law at West Virginia University College of Law.

Jordan "Jody" M. Blanke is the Ernest L. Baskin, Jr. Distinguished Professor of Computer Science and Law at Mercer University.

Robert M. Bloom is a Professor of Law at Boston College Law School.

Jenny E. Carroll is the Wiggins, Childs, Quinn and Pantazis Professor of Law at the University of Alabama School of Law.

Kami Chavis is a Professor of Law, Associate Provost for Academic Initiatives, and Director of the Criminal Justice Program at Wake Forrest University School of Law.

Morgan Cloud is the Charles Howard Candler Professor of Law at Emory University School of Law.

Daniel T. Coyne is a Clinical Professor of Law at the Illinois Institute of Technology/Chicago-Kent College of Law.

Dr. William Cuddihy is an Adjunct Associate Professor of History at Los Angeles City College.

Steven Duke is a Professor of Law at Yale Law School.

Norman M. Garland is a Professor of Law at Southwestern Law School.

Catherine M. Grosso is an Associate Professor of Law at Michigan State University College of Law.

M. Eve Hanan is an Associate Professor of Law at the William S. Boyd School of Law, University of Nevada-Las Vegas.

Janet C. Hoeffel is the Catherine D. Pierson Professor of Law at Tulane University.

Andrew Horwitz is the Assistant Dean for Experiential Education at the Roger Williams University School of Law.

Justin Marceau is a Professor of Law at the University of Denver-Sturm School of Law.

Michael Meltsner is the Matthews Distinguished University Professor of Law at Northeastern University.

Colin Miller is a Professor and Associate Dean for Faculty Development at the University of South Carolina School of Law.

Luke Milligan is a Professor of Law at the Louis D. Brandeis School of Law, University of Louisville.

William P. Quigley is a Professor of Law at Loyola University New Orleans.

Larry J. Ritchie is a Professor of Law at Roger Williams University School of Law.

Amy D. Ronner is a Professor of Law at St. Thomas University School of Law.

Christopher Slobogin is the Milton R. Underwood Chair at Vanderbilt University Law School.

Mary Pat Treuthart is a Professor of Law at Gonzaga University School of Law.