14-2985-cv

United States Court of Appeals

for the

Second Circuit

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

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

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

BRIEF FOR *AMICI CURIAE* BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, AMERICAN CIVIL LIBERTIES UNION, THE CONSTITUTION PROJECT, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT

FAIZA PATEL
MICHAEL PRICE
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Sixth Avenue, 12th Floor
New York, New York 10013
(646) 292-8335

Attorneys for Brennan Center for Justice at NYU School of Law

BRETT J. WILLIAMSON
DAVID K. LUKMIRE
NATE ASHER
O'MELVENY & MYERS LLP
Times Square Tower
Seven Times Square
New York, New York 10036
(212) 326-2000

Attorneys for Amici Curiae Brennan Center for Justice at NYU School of Law and The Constitution Project

(For Continuation of Appearances See Inside Cover)

HANNI FAKHOURY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333

ALEX ABDO
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, New York 10004
(212) 549-2500

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

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, including access to the courts and constitutional limits on the government's exercise of power. 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 counterterrorism policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on privacy and First Amendment freedoms. As part of this effort, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S .Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp*., 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008).

[1] This *amicus* brief is filed with the consent of all parties to this proceeding. No party's counsel authored any portion of this brief. No party or party's counsel contributed money intended to fund this brief's preparation or submission. 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.

The American Civil Liberties Union is a nationwide, nonprofit, nonpartisan organization with over 500,000 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 Constitution Project (TCP) is a constitutional watchdog that brings together legal and policy experts from across the political spectrum to promote and defend constitutional safeguards. TCP's bipartisan Liberty and Security Committee, founded in the aftermath of September 11th, is composed of policy experts, legal scholars, and former high-ranking government officials from all three branches of government. This diverse group makes policy recommendations to protect both national security and civil liberties, for programs ranging from government surveillance to U.S. detention. Based upon their reports and recommendations, TCP files amicus briefs in litigation related to these issues.

TCP's Liberty and Security Committee has published several reports addressing the Fourth Amendment and government access to and use of data. In the committee's "Report on the FISA Amendments Act of 2008," the members evaluated the unique Fourth Amendment concerns presented by government

surveillance in the digital age and recommended "stronger safeguards restricting government retention and use of private communications." In the reports "Principles for Government Data Mining," and "Recommendations for Fusion Centers," the committee emphasized the importance of due process in government data collection and issued sets of recommendations that would allow the government to protect the civil liberties of citizens while combating crime and terrorism.

Additionally, TCP is a member of the Digital Due Process coalition. A core principle of this coalition is that a warrant is required for obtaining the content of private communications such as emails: "[t]he government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online."

The Electronic Frontier Foundation (EFF) is a member-supported civil liberties organization working to protect innovation, free speech, and privacy in the digital world. With approximately 23,000 dues-paying members nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has served as amicus curiae in landmark privacy cases addressing Fourth Amendment issues raised by emerging technologies, as well as cases involving the application of the Stored Communications Act. *See, e.g.*, *Riley*, 134

S. Ct. 2473; *United States v. Jones*, 132 S. Ct. 945 (2012); *City of Ontario v. Quon*, 560 U.S. 746 (2010); *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 306 (3d Cir. 2010).

SUMMARY OF ARGUMENT

This is a cautionary brief. Whatever the outcome of this appeal, the panel should not rely on the district court's reasoning in reaching its decision. The lower court made two errors, which, if upheld, would have far-reaching consequences for the future of digital privacy.

First, the court reasoned that the Fourth Amendment does not apply to copying data, only to searching it. *Amici* believe this position is fundamentally misguided. The Fourth Amendment "moment" occurs at the point the data is copied and produced to law enforcement, regardless of when or whether an officer might look at it. A contrary view would vitiate the Fourth Amendment's protections in the digital age. It would, for example, permit the police to copy every file on every computer used by every judge on this Court, no warrant required.

Second, the lower court reasoned that the Government can use a warrant to search and seize email abroad because it is somehow similar to a subpoena. That logic ignores the constitutional limitations of subpoenas, which are insufficient instruments to compel the disclosure of email—in the United States or elsewhere. *Amici* urge the Court to reject the Government's analogy to subpoenas. That rationale, if adopted, would imply that a mere subpoena is adequate for American law enforcement to access American email, contrary to the history and purpose of the Fourth Amendment.

For these reasons, *Amici* urge the Court to approach this case with caution and avoid the errors below.

ARGUMENT

I. The Fourth Amendment "Moment" Happens at the Point of Collection.

The district court erred in reasoning that copying email does not trigger the Fourth Amendment. Instead of recognizing the act as a potential seizure, it found that the Fourth Amendment "moment" does not occur until the Government actually searches through the records in the United States. The court relied on this error to conclude that the warrant in question, obtained by the Government under the Stored Communications Act, 18 U.S.C. §§ 2701–2712 ("SCA"), "does not implicate principles of extraterritoriality." SA 12. But as expedient as this argument may be, it is also deeply flawed. The court did not adequately consider

the Fourth Amendment's distinct protection against unreasonable seizures. Longstanding Fourth Amendment analysis dictates a finding in this case that the seizure of data will occur as soon as Microsoft, acting as the government's agent, copies the data in question.

A. Copying Data Is a Seizure.

The district court erred in accepting the Government's argument that a Fourth Amendment event does not occur until government agents actually search the records in question. Rather, *Amici* submit that the constitutional moment occurs when Microsoft copies customer data at the behest of the Government.

1. The Government Conscripted Microsoft.

Microsoft acts on behalf of the Government by executing an SCA warrant. For Fourth Amendment purposes, it is irrelevant that a Microsoft technician, and not an FBI agent, is responsible for actually clicking the buttons and copying the data. A search or seizure by a third party acting on behalf of the government is still a search or seizure. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984); *Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) ("It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search."). Even the SCA anticipates that law enforcement will call on service providers to perform this function. *See* SCA

§ 2703(g) (stating that the presence of an officer "shall not be required" for service or execution of an SCA warrant). The need for Microsoft's cooperation is hardly surprising given the technical expertise required to identify and copy specific data from its global network. And it is far preferable to have Microsoft seize the data than to have an FBI team storm Microsoft's datacenter. The Government, though, remains the instigator. *See Cassidy*, 471 F.3d at 74 ("…a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment").

2. Copying Data Infringes on the Owner's Possessory Interests and Is Therefore a Seizure.

Because Microsoft is acting as the Government's agent, the question becomes whether copying customer data and transmitting it to the Government is a Fourth Amendment search or seizure. The district court found that it was not, based primarily on assertions in a law review article that have now been reconsidered by the author. SA 12–13 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005)).[2] *Amici* believe the district court erred on this point and urge this panel to not to repeat its mistake.

[2] Critically, Professor Kerr later reversed himself, explaining that he first "reasoned that the intuitively necessary limitations on [copying electronic data] should come from the Fourth Amendment's regulations on searches instead of seizures," but "I now see that my earlier approach was wrong . . . ." Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 714 (2010). Professor

The district court wrongly accepted the Government's argument that the "mere gathering of data by a provider in anticipation of disclosing it to law enforcement is not a 'seizure.'" Government's Brief in Support of the Magistrate Judge's Decision at 15 n.8 (Dkt. No. 60), *In Re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, 2014 WL 4629624 (S.D.N.Y. 2014) (Nos. M9-150, 13-MJ-2814) (hereinafter "Gov't Brief in Support"). Indeed, just six months ago this Court explained that data copied from hard drives was seized when the copying occurred. *See United States v. Ganias*, 755 F.3d 125, 135–36 (2d Cir. 2014). This position is consistent with other circuits. *See United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (referring to the copying of electronic data as a seizure throughout the opinion); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (describing information retrieved by Yahoo! technicians from two e-mail accounts as a "seizure"). Copying data at the Government's behest is a Fourth Amendment event.

The Government's argument gives no consideration to the possessory interests of the individual whose property is being seized. As the Supreme Court has explained, "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United*

Kerr now analyzes the copying of data as a seizure, as described further below, and this Court should do the same.

Jacobsen, 466 U.S. at 113. The Government's position—that duplicating a person's email does not "meaningfully interfere" with a possessory interest in those communications—mischaracterizes the impact on the property owner. In the case of intangible property such as electronically stored data, which can be easily duplicated in identical form, meaningful interference occurs the moment the property is copied. *See* Kerr, 119 Yale L.J. at 712 ("Given the importance of data, and the frequent existence of multiple copies of it, there is little difference between (a) taking a physical device that contains data and (b) copying the data without taking the device.").

This position is consistent with the Supreme Court's standard that a seizure occurs as soon as there is meaningful interference with a possessory interest, and with the purpose of regulating seizures under the Fourth Amendment. *See* Kerr, 119 Yale L.J. at 703, 711 ("copying data 'seizes' it under the Fourth Amendment when copying occurs without human observation and interrupts the course of the data's possession or transmission," since copying "interferes with the owner's right to control the item seized"); *see also In re A Warrant for All Content and 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 a seizure).[3]

An analogy to the right of exclusive possession accorded by our intellectual property laws reinforces the view that copying a person's electronic data meaningfully interferes with possessory rights in that property, even without further observation or disclosure. Both intellectual property law and Fourth Amendment law focus on owners' control over their property. Specifically, first among the enumerated rights in the Copyright Act is the exclusive right to copy one's own work. *See* 17 U.S.C. § 106 ("the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies . . . ."). This right is not conditional; verbatim copying without permission is per se actionable as infringement. *See Hoehling v. Universal City Studios, Inc.*, 618 F.2d 972, 980 (2d Cir. 1980); *SHL Imaging, Inc.*

[3] The Government's only contrary authority is a District of Oregon case, *In re Application of the United States*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009), the holding of which is in direct conflict with the subsequent *Comprehensive Drug Testing* case from the Ninth Circuit that characterized copied data as "seized data." *Comprehensive Drug Testing*, 621 F.3d at 1168–71; *See* Kerr, 119 Yale L.J. at 708–709 (discussing *Comprehensive Drug Testing*).

v. Artisan House, Inc., 117 F. Supp. 2d 301, 318 (S.D.N.Y. 2000) ("In summary, the undisputed evidence shows that the photographs are entitled to copyright protection; that plaintiff is the sole owner of the copyrights in those photographs; and defendants copied the photographs verbatim without the authority of the copyright owner. Accordingly, defendants are liable for infringing plaintiff's copyrights.").[4]

Infringement does not hinge on whether the protected work is ever "used" by the infringing party. The essence of one's ownership right is the right to exclude others from accessing it. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006). Thus infringement occurs at the moment of willful duplication, regardless of the purpose. *Rosner v. Codata Corp.*, 917 F. Supp. 1009, 1018 (S.D.N.Y. 1996) ("when a defendant copies a plaintiff's work, the infringement occurs at the moment of copying . . . "); *see also Auscape Int'l v. Nat'l Geographic Soc'y*, 409 F. Supp. 2d 235, 247, 253 (S.D.N.Y. 2004) (plaintiff suffers injury, for purposes of accrual of a cause of action, at the moment of infringement).

Contrary to the Government's bald assertion that no "seizure" takes place until the property "enters the Government's possession," the Fourth Amendment "moment" occurs as soon as the Government's action impacts the owner. *See Jacobsen*, 466 U.S. at 113, n.5 ("While the concept of a 'seizure' of property is not

[4] Notably, mere "reproduction" of just a single copyrighted work also exposes the copier to criminal penalties. *See* 17 U.S.C. § 506(a)(1)(B).

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). The same interests at play in copyright law—including the owner's ability to preserve control over his electronic files—mandate this conclusion.

B. 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 the Government actually examines copied data is at odds with existing law and the fundamental purposes of the Fourth Amendment.

First, it is in tension with established principles of copyright law, as detailed above, including precedent from this Court. Second, it is inconsistent with the law governing other forms of electronic surveillance. For instance, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act") generally prohibits the interception of wire and electronic communications, defined as the "*acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4) (emphasis added). There is no requirement that law enforcement actually look at the data.

A contrary ruling in this case could have far-reaching consequences. For example, the panel may unintentionally endorse a "seize first, search later" view of the Fourth Amendment, but that view would lead to absurd results: Under this view, a warrant would not be required for the Government to copy and keep *all* electronic communications stored on a device associated with the target of the warrant—a concern this Court recently identified in *Ganias*. 755 F. 3d at 137 ("If the . . . warrant authorized the Government to retain . . . data . . . on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a[n illegal] general warrant.").[5] And by the same token, the Government could seize a computer, copy all of its data (communications and otherwise), and maintain that information indefinitely—all without a warrant.

This is not idle speculation. Although the SCA is nominally limited to "communications," the district court ordered Microsoft to turn over not only individual emails, but "*[a]ll records or other information* stored by an individual using the account, including address books, contact and buddy lists, pictures, and files." SA 4 (emphasis added). The government's own request underscores that with the advent of "cloud computing," a user's email account contains not just

[5] Indeed, because there is no rational basis to justify the Government's distinction between such a seizure and seeking property from physical premises, this argument would also "permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until agents haul it off to the [warrant's] issuing district." *In re Warrant to Search Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013).

individual messages and their subject lines, but it may also contain vast archives of personal information, including financial and medical records. *See Riley*, 134 S . Ct. at 2491 (2014). If there is no Fourth Amendment intrusion until a human being actually examines copied data, then the Government could collect data belonging to anyone, without a warrant, just in case it might be useful at some later point. Following this logic, federal agents could copy the hard drives belonging to every member of this Court and never need to seek a warrant unless they want to peruse the contents.

Accepting the Government's position could also embolden foreign governments to access American data under far weaker standards than those applicable in this country. If, as the Government maintains, there is no privacy infringement at the point data is copied or collected, then foreign governments may feel inspired to reciprocate by copying any American data within their reach.

As Microsoft stated at oral argument below, these concerns are not conjecture. Chinese officials have already approached the company seeking emails belonging to Americans. *See* Tr. of Oral Arg. (July 31, 2014), *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.* (hereinafter "Tr.") at 51. And less than six months ago, the British Parliament passed a law requiring Internet and telephone companies to collect users' personal data and hand it over to up to 600 government agencies

upon request. *See* Drip surveillance law faces legal challenge by MPs, *The Guardian* (July 22, 2014), *available at* http://www.theguardian.com/world/2014/jul/22/drip-surveillance-law-legal-challenge-civil-liberties-campaigners. If this panel adopts the Government's reasoning, technology companies would have weaker grounds to oppose demands from foreign government for information belonging to United States persons. SA 30 (quoting Restatement (Third) of Foreign Relations § 442 (1)(a)). The result would leave millions of Americans who do business with globally operated ISPs vulnerable to foreign surveillance.

II. The Court Should Not Rely on the Government's Analogy to Subpoenas

The Government argues that it has the power to seize emails in Ireland using a domestic warrant because it could also do so with a domestic subpoena. *See* Gov't Brief in Support at 5–6. That is wrong. A subpoena is constitutionally insufficient to require the disclosure of email in the United States, let alone in Ireland. *See Warshak*, 631 F.3d at 285 286. This panel should not accept or endorse any position to the contrary. If a warrant is sufficient to compel the disclosure of email abroad, it must be for some other reason. The Government's analogy to subpoenas is misplaced.

A. The Government Relies on an Incorrect Assumption about Its Subpoena Authority.

The Government relies on its subpoena authority under the Stored Communications Act to argue that an "SCA warrant" applies to email stored

outside the United States. *See* Gov't Brief in Support at 4–16. It imagines an "upside-down pyramid" where information accessible with a subpoena must also be accessible with a warrant. *Id.* at 6. But the Government ignores recent rulings by the Supreme Court and the Sixth Circuit Court of Appeals that undermine the building blocks of this argument. *See Riley*, 134 S. Ct. at 2489; *Warshak*, 631 F.3d at 286. In short, bricks are missing from the pyramid.

The Government goes to great lengths to liken an SCA warrant to a subpoena. It argues that SCA warrants are "functionally similar to subpoenas" Gov't Brief in Support at 8. *See also id.* at 7 (citing *Email Account Controlled and Maintained by Microsoft Corp*, 15 F. Supp. 3d at 471 (Francis, MJ)); *id*. at 10 ("[T]he Government is exercising a power to compel the provider to produce records in its possession, subject to judicial sanction, as entailed in a subpoena."). Consequently, it contends, all of the records available with a subpoena should also be available with warrant. *Id.* at 6.

The Government's rationale for pressing this analogy is the *Bank of Nova Scotia* doctrine, which holds that the foreign origin of documents "should not be a decisive factor" in determining whether to enforce a subpoena. 740 F.2d 817, 828 (11th Cir. 1984). On this basis, the Government argues, if a subpoena can reach records located abroad, then so too can a warrant. Gov't Brief in Support at 12, 16.

This analogy fails, however, with respect to email stored by a third party service provider—in this case, Microsoft. A subpoena may be used to compel disclosure of certain business records. Those records entail basic subscriber data such as a user's name, address, length of service, and billing information. *See* 18 U.S.C. § 2703(c)(2).[6] Microsoft produced this information. *See* Microsoft's

[6] There is currently disagreement about whether certain forms of "metadata," such as email routing data, "to/from" information, and location information are truly "business records" available to law enforcement with a subpoena. A growing number of courts have recognized the intensely private nature of this information and have required police to obtain a warrant before accessing it. *See, e.g., United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014), *reh'g en banc granted*, 573 F. App'x 925 (2014) (finding and expectation of privacy in historical cell site information notwithstanding the fact the data is exposed to the phone company); *In re Application of the United States for an Order Directing a Provider of Elec. Commc'ns*, 620 F.3d 304, 317–18 (3d Cir. 2010) (phone customer has not necessarily disclosed cell site location information to law enforcement and thus magistrate may require government use probable cause warrant to obtain records); *United States v. Powell*, 943 F. Supp. 2d 759, 778 (E.D. Mich. 2013) (expectation of privacy in real time cell site tracking records and requiring probable cause warrant); *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 125 (E.D.N.Y. 2011) (finding that "there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private" and concluding that an exception to the third-party doctrine applies to cell-site-location records); *Tracey v. State*, — So. 3d —, No. SC11-2254, 2014 WL 5285929, at *16 (Fla. Oct. 16, 2014) (expectation of privacy in real time cell site information notwithstanding the fact the records are disclosed to the phone company for "to a business or other entity for personal purposes"); *Commonwealth v. Augustine*, 4 N.E. 3d 846, 863 (Mass. 2014) (even though historical cell site information is "business information" privacy interests require police obtain a search warrant to obtain them); *State v. Earls*, 70 A.3d 630, 644 (N.J. 2013) (expectation of privacy in historical cell site information notwithstanding the fact the records are exposed to the phone provider); *see also State v. Reid*, 945 A.2d 26, 35§36 (N.J. 2008)

Objections to the Magistrate's Order at 9 (Dkt. No. 15), *E-mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 13 Mag. 2814). But the Fourth Amendment requires more than a subpoena for email stored on a customer's behalf.

B. Subpoenas Are Constitutionally Insufficient to Obtain Email

The SCA can compel a service provider to disclose the contents of stored electronic communications under certain circumstances. But to the extent the SCA authorizes the Government to do so with a subpoena, it is unconstitutional. *See Warshak*, 631 F.3d at 286.

The Fourth Amendment explicitly protects private "papers" from unreasonable searches and seizures. U.S. Const. amend. IV. And the Supreme Court has recognized that the Framers intended to protect the privacy of written communications as much as a diary tucked under the bed. *See United States v. Jacobsen*, 466 U.S. 109, 114–15 (1984) (holding that there is a legitimate expectation of privacy in letters and other sealed packages); *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) ("Whilst in the mail, [letters] can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly

---

(expectation of privacy in Internet subscriber information requires police use grand jury subpoena to obtain them); *but see, e.g., In re Application for Historical Cell Site Data*, 724 F.3d at 613 (no expectation of privacy in historical cell site information); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (no expectation of privacy in Internet subscriber information).

describing the thing to be seized, as is required when papers are subjected to search in one's own household."); *Entick v. Carrington*, 19 How. Str. Tr. 1029, 1064, 95 Eng. Rep. 807 (C.P. 1765) ("[I]f this point should be determined in favor of the jurisdiction, the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."). One's digital papers (such as email) should enjoy at least as much constitutional protection as a letter delivered by the post office.

The Sixth Circuit endorsed this conclusion in *Warshak*, reasoning that email "is the technological scion of tangible mail" and that it would "defy common sense to afford emails lesser Fourth Amendment protection." 631 F.3d at 285–86 (citing *City of Ontario v. Quon*, 560 U.S. 746, 762–63 (2010) ("implying that 'a search of [an individual's] personal e-mail account' would be just as intrusive as 'a wiretap on his home phone line'"). *See also United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("holding that '[t]he privacy interests in [mail and email] are identical'")).

Warshak likened service providers to "the functional equivalent of a post office or a telephone company." 631 F.3d at 286. Compelling a service provider to surrender the contents of a subscriber's emails is therefore a Fourth Amendment

search, "which necessitates compliance with the warrant requirement absent some exception." *Id.*

Warshak is consistent with the Supreme Court's emerging approach to the Fourth Amendment in the digital age. In *United States v. Jones*, Justice Sotomayor questioned the continued viability of the so-called "third party doctrine," which holds that there is no privacy interest in information knowingly and voluntarily revealed to "third parties," such as a bank or telephone company. *See United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979). Sotomayor called the doctrine "ill suited to the digital age" and suggested that it may be necessary to reconsider the premise altogether. *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

Indeed, the third party doctrine has never been absolute. The Court has declined to extend the logic to medical records. *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (finding that the typical patient undergoing diagnostic tests in a hospital has a reasonable expectation of privacy that the results of those tests will not be shared with nonmedical personnel without her consent). And of course, the Court has long held that the Fourth Amendment protects the privacy of letters in the mail. *See Ex Parte Jackson*, 96 U.S. at 733.

But especially in recent years, the third party doctrine has encountered a growing chorus of criticism as people live more of their lives online. *See United*

States v. Davis, 754 F.3d 1205, 1216–1217 (11th Cir. 2014), *reh'g en banc granted*, 573 F. App'x 925 (11th Cir. 2014) (finding a reasonable expectation of privacy in cell phone location records stored by a cell phone provider); *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (recognizing that emails "are expected to be kept private and this expectation is one that society is prepared to recognize as reasonable"); *In re Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records*, 620 F.3d at 317–18 (recognizing that cell phone users do not "voluntarily" share their location information with service providers in any meaningful way); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2007) (finding no expectation of privacy in email logs but reserving right to reconsider the issue when it comes to "content"); *see also* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614, 619, 680 (2011); Patricia L. Bellia & Susan Friewald, *Fourth Amendment Protection for Stored Email*, U. Chicago Legal Forum, 121, 147–149 (2008); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975, 977 (2007); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1086, 1138 (2002).

Modern technology has dramatically expanded the reach of the doctrine far beyond records of bank transactions and telephone calls. The Supreme Court recognized this problem in *Riley*, reasoning that Fourth Amendment privacy protection must account for this new technological reality. There, in holding that cell phones may not be searched under the search-incident-to-arrest warrant exception, the court noted that modern cell phones—just like cloud-based email—are capable of storing a vast amount of personal information and thus deserve the highest privacy protections:

> Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: 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 . . . .

Riley, 134 S. Ct. at 2491. What the Supreme Court wrote about cell phones applies equally to email: modern email contains "[t]he sum of an individual's private life," including "a record of all his communications," and materials such as prescriptions and bank statements. *Id.* at 2489. The concerns animating *Riley* apply equally here and strongly support the position that law enforcement access to email requires a warrant supported by probable cause, not a simple subpoena.

In sum, a subpoena is constitutionally insufficient to search and seize mail, physical or electronic. The Government's reliance on its subpoena authority and the *Bank of Nova Scotia* doctrine is therefore misplaced. Even if a subpoena is

sufficient to compel the production of a service provider's business records, it is no substitute for a warrant and it offers no analogous authority to reach email content —one's electronic papers—stored abroad.

Of course, the Government did get a warrant, and *Amici* do not dispute that it is constitutionally sufficient to compel Microsoft to disclose email content located in the United States. But the question is whether an SCA warrant applies to email located abroad. In this respect, the *Bank of Nova Scotia* doctrine is of no assistance; subpoenas extend only to business records, not to the stored communications of customers. *Warshak*, 631 F.3d at 286–88. And if subpoenas do not reach stored communications, then the Government's argument falls apart.

A bank, for example, may be required to produce its own business records pursuant to a subpoena, even if those records are located abroad. *See Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983). But a subpoena will not suffice to search the contents of a safe deposit box belonging to a customer. *See United States v. First Nat'l Bank*, 568 F.2d 853, 858 (2d Cir. 1977) (recognizing that the search of safe deposit box falls within the scope of the Fourth Amendment). Likewise here, a customer's emails are not Microsoft's business records. They are private communications, secured in a digital lockbox, and therefore inaccessible with a subpoena.

Microsoft stores private data in trust for its customers. The data does not belong to Microsoft any more than the bank owns the contents of a safe deposit box. Microsoft may have a key, but it has no business interest in the contents; it does not matter if emails are full of gibberish or Shakespeare. Like a landlord or a storage company, there is a business interest in receiving the rent on time, not in the tenant's belongings. Thus, the relevant business records might include contact and billing information, but not the contents of the storage locker or apartment. A warrant is required to search that property. *See United States v. Karo*, 468 U.S. 705, 720 n.6 (1984) (recognizing that an individual "surely . . . [has] a reasonable expectation of privacy in their own storage locker" and that revealing its contents would constitute a search).

Even if this Court determines that SCA warrants apply extraterritorially, it should not do so relying on the inapt analogy to subpoenas. The comparison is misguided in this digital age and, if adopted, could unintentionally endorse a principle that is odious to privacy and the Fourth Amendment.

To be sure, a warrant is more substantial than a subpoena. But in this case, there is considerable doubt about what that yields. The *Warshak* court found that a subpoena is insufficient to compel the production of email from a service provider. 631 F.3d at 286. And the Supreme Court has twice indicated that it would agree. *See Riley*, 134 S. Ct. at 2491; *Jones*, 132 S. Ct. at 957. The heightened privacy

interests at stake demand greater vigilance when assessing the reasonableness of warrantless intrusions into our digital data. *See Quon*, 560 U.S. at 759 (cautioning jurists to "proceed with care when considering the whole concept of privacy expectations in [electronic] communications"). The authority for a U.S. search warrant to reach data stored abroad must stand on its own two feet, and not on the flawed premise that the same information is available by subpoena.

CONCLUSION

No matter how this Court rules, it should not rely on the district court's flawed reasoning. It should continue to insist that copying data is a seizure and find that the Fourth Amendment" 'moment" occurs at the point of collection. And this Court should not rely on the Government's inapt analogy to subpoenas. Both of these issues have tremendous ramifications for digital privacy and the future of the Fourth Amendment. *Amici* urge the Court to carefully consider those possible consequences.

Dated: December 15, 2014

Respectfully submitted,

/s/ Michael Price

Faiza Patel
Michael Price
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
161 6th Ave., 12th Floor
New York, New York 10012
(646) 292-8335
Counsel for Brennan Center for Justice at NYU School of Law

Brett J. Williamson
David K. Lukmire
Nate Asher
O'MELVENY & MYERS LLP
7 Times Square
New York, NY 10036
(212) 326-2000

Counsel for Amici Curiae Brennan Center for Justice at NYU School of Law and The Constitution Project

Alex Abdo
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(a)(7)(C) of the Federal Rules of Appellate Procedure, I certify that, according to the word-count feature of the word processing program, this brief contains 6,354 words and therefore is in compliance with the type-volume limitation set forth in Rule 32(a)(7)(B).

/s/ Michael Price
Michael Price

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system on December 15, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Michael Price
Michael Price

Counsel for Brennan Center for Justice at NYU School of Law