Case No. 18-1306

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

PATRICK HATELY, an individual,

Plaintiff-Appellant,

v.

DR. DAVID WATTS, an individual,

Defendant-Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

BRIEF OF AMICI CURIAE THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE ELECTRONIC FRONTIER FOUNDATION, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

Marta F. Belcher (*counsel of record*)
James R. Batchelder
Monica A. Ortel
James H. Rickard
ROPES & GRAY LLP
1900 University Avenue, 6th Floor
East Palo Alto, CA 94303
(650) 617-4000

Evan Gourvitz
Lance W. Shapiro
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036
(212) 596-9000

Kathryn C. Thornton
ROPES & GRAY LLP
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
(202) 508-4600

Gregory T. Nojeim
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street NW, Suite 200
Washington, D.C. 20005
(202) 637-9800

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

Kevin Bankston
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE
740 15th Street NW, Suite 900
Washington, D.C. 20036
(202) 986-2700

Attorneys for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 18-1306 Caption: PATRICK HATELY v. DR. DAVID WATTS

Pursuant to FRAP 26.1 and Local Rule 26.1,

The Center for Democracy & Technology, the Electronic Frontier Foundation, and
(name of party/amicus)

New America's Open Technology Institute

who is amici curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: *\/s\/ Marta F. Belcher* Date: May 29, 2018

Counsel for: amici curiae

CERTIFICATE OF SERVICE

****

I certify that on May 29, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Marta F. Belcher
(signature)

May 29, 2018
(date)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Constitution

Statutes

Legislative History

Other Authorities

INTEREST OF AMICI CURIAE[1]

The Center for Democracy and Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the internet and other communications networks. CDT represents the public's interest in an open, decentralized internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty. CDT assembled and is leading the Digital Due Process coalition, which is dedicated to updating the Electronic Communications Privacy Act ("ECPA").

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or amicus in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the internet and other new technologies. With roughly 40,000 dues-paying members, 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.

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), amici certify that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money intended to fund the brief's preparation or submission; and no person other than amici and their counsel contributed money intended to fund the brief's preparation or submission.

New America's Open Technology Institute ("OTI") is New America's program dedicated to ensuring that all communities have equitable access to digital technology and its benefits, promoting universal access to communications technologies that are both open and secure. New America is a Washington, D.C.-based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age. OTI works to ensure that government access to electronic communications is subject to robust safeguards for cybersecurity and individual privacy.

SUMMARY OF ARGUMENT

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), including its Title II, the Stored Communications Act ("SCA"), to protect electronic communications from unauthorized access, and to extend Fourth Amendment-like privacy protections to electronic communications held by third-party service providers. Three decades later, these electronic communications—such as email, text messaging, and social media messaging—have become a ubiquitous part of everyday life, and these privacy protections are more important than ever.

However, the district court's decision in this case would strip these communications of the protections of ECPA and the SCA ***as soon as they are opened***. Paradoxically, spam and other unwanted, unopened messages would retain these vital privacy protections, while the most intimate and important personal communications would no longer enjoy SCA protections against unauthorized access by individuals, the government, and other entities.[2] Furthermore, because other circuits have correctly held that opening an electronic communication does ***not*** deprive it of the protections of ECPA and the SCA, affirming the district court's

[2] Regardless of SCA protections, personal communications are also protected against government access by the Fourth Amendment to the U.S. Constitution, and are also protected against unauthorized access by the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

decision would provide electronic communications with different levels of protection in different states, and as people travel between states, undermining the fundamental purpose of ECPA and the SCA. Accordingly, this Court should reverse the district court's summary judgment that, because they had been opened, the emails in this case were not "in electronic storage" for the purposes of the SCA.

ARGUMENT

I. Background

A. The Stored Communications Act and Electronic Communications Privacy Act protect digital communications from unauthorized access by individuals and the government

In 1986, in light of technological advancements such as the advent of email, Congress passed the Electronic Communications Privacy Act in response to concerns that electronic communications were inadequately protected from unauthorized access. Through its three titles, ECPA regulates (i) the interception of communications, (ii) the access to or disclosure of electronic information stored with service providers, and (iii) the use of pen registers and similar surveillance devices. S. Rep. No. 99-541, at 3 (1986). Title II of ECPA, the Stored Communications Act, "criminalizes unauthorized access to users' stored communications, restricts Internet service providers from voluntarily sharing those communications, and regulates the government's ability to request user data from those providers." Gabriel R. Schlabach, *Note*, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 693 (2015) (footnotes omitted). The

SCA also provides a private civil remedy for violations of its protections.[3] 18 U.S.C. § 2707(a). To qualify for SCA protection, an electronic communication must be in "electronic storage," defined as, (A) "any temporary intermediate storage . . . incidental to [] electronic transmission," or (B) "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

B. The district court's holding in this case would strip electronic communications of vital privacy protections the moment they are opened

In *Hately*, the district court concluded that ECPA's definition of "electronic storage" in § 2510(17) covers only communications that have not been downloaded or read. *See Hately v. Watts*, No. 1:17-cv-00502-AJT-JFA, slip op. at 5 (E.D. Va. Mar. 14, 2018). The court's interpretation of "electronic storage" does not encompass any communication stored, for example, in a user's email inbox, on a text messaging service, or in a social media account ***once it has been opened***. The court found that, once opened, these communications are no longer in "temporary, intermediate storage . . . incidental to the[ir] electronic transmission" under the first

[3] ECPA distinguishes between providers that offer an Electronic Communication Service ("ECS") and a Remote Computing Service ("RCS"). An ECS allows for the sending or receiving of electronic communications, 18 U.S.C. § 2510(15), while an RCS provides storage or processing services, 18 U.S.C. § 2711(2). The provision at issue here applies to ECS service providers. *See Hately v. Watts*, No. 1:17-cv-00502-AJT-JFA, slip op. at 5, 8-9 (E.D. Va. Mar. 14, 2018).

prong of § 2510(17)(A)'s definition of "electronic storage," nor are they in storage "for purposes of backup protection of such communication" under the second prong of the definition. *See Hately*, slip op. at 4-5 (E.D. Va. Mar. 14, 2018). Regarding the second prong, the district court held that "the 'backups' in paragraph (B) are most logically and reasonably read as referring only to backups of the transitory communications described in paragraph (A), created and stored separate and apart from the copies maintained to facilitate continuing access by the user through his account." *Id.* at 9. That is, the court interpreted "any storage of such communication by an electronic communication service for purposes of backup protection of such communication" to include only backups of communications after they have been delivered but remain unread, excluding all backups of those same communications ***once they have been read***.

C. The district court's erroneous reading of "electronic storage" contradicts other courts' interpretations of the term

The district court's narrow interpretation of "electronic storage" is at odds with rulings and compelling reasoning from multiple circuits that have addressed this issue. While the Eighth Circuit has found that copies of sent emails retained on an email server "as a matter of course" are not stored "for purposes of backup protection," other circuits have taken an expansive view of "electronic storage" that provides protection consistent with the legislative intent behind the SCA. *See Anzaldua v. Ne. Ambulance & Fire Protection Dist.*, 793 F.3d 822, 839 (8th Cir.

2015) (adopting a narrow view of "electronic storage" when determining that a draft email and a copy of a sent email were not "in electronic storage"). For example, the Ninth Circuit held in *Theofel v. Farey-Jones* that "messages remaining on an [internet service provider]'s server after delivery" were stored "for purposes of backup protection" because they "function[] as a 'backup' ***for the user***." 359 F.3d 1066, 1075 (9th Cir. 2004) (emphasis added). The Ninth Circuit explained that "prior access is irrelevant to whether the messages at issue were in electronic storage." *Id.* at 1077. Thus, for purposes of § 2510(17)(B) the Ninth Circuit found that "an email maintained by an internet service provider ('ISP') is held 'for the purposes of backup protection,' and therefore is 'in electronic storage,' so long as the user has not deleted the service copy[4] 'in the normal course,' regardless of whether the storage copy was made when the email was 'in transit.'" *See Hately*, slip op. at 8 (E.D. Va. Mar. 14, 2018) (quoting *Theofel*, 359 F.3d at 1076). *Theofel* also explicitly rejected the district court's reasoning in this case that the "backups" in paragraph (B) refer only to the backups of the transitory communications described in paragraph (A). *See Theofel*, 359 F.3d at 1075. As the district court acknowledged, courts outside the Ninth Circuit have adopted similar reasoning to *Theofel*. *Hately*, slip op. at 8 (E.D. Va. Mar. 14, 2018) (citing *Pure Power Boot*

[4] As explained in Section II.D., the distinction between the "service copy" of an email and "backup storage copies" is a false one that cannot be squared with the way that modern electronic communications services operate.

Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 556 (S.D.N.Y. 2008); *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156 (E.D. Mich. Feb. 6, 2008)); *see also Theofel*, 359 F.3d at 1075 (collecting cases). Similarly, the First Circuit (en banc) adopted a broad definition of "electronic storage" covering messages "stored in a user's mailbox." *United States v. Councilman*, 418 F.3d 67, 77, 81 (1st Cir. 2005).

D. Congress enacted ECPA and the SCA to protect the privacy of electronic communications, to codify Fourth Amendment-like rights for communications stored by third parties, and to promote technological advancement

The district court's ruling undermines Congress's intent in enacting ECPA and the SCA. The legislative history of ECPA reflects that Congress enacted the SCA in response to concerns that legal and technical protections were insufficient to protect the privacy of sensitive and intimate electronic communications such as emails:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations . . . . But there are no comparable Federal statutory standards to protect the privacy and security of new noncommon carrier communications services or new forms of telecommunications and computer technology.

S. Rep. No. 99-541, at 5 (1986).

Accordingly, Congress sought to provide a baseline of privacy protection for electronic communications by extending Fourth Amendment-like rights to such communications stored by third-party service providers. Congress also sought to promote technological advancement by allowing users to trust in the privacy of then-novel services such as email.

Moreover, the legislative history reflects that Congress intended to protect these communications where and when they are most vulnerable—while stored in the user's mailbox. Senator Leahy, the leading proponent of ECPA in 1986, as amicus in *Councilman*, explained that "what Congress certainly did intend by protecting stored communications was to guard against unauthorized access to communications at a point where they were perceived to be particularly vulnerable: in the user's mailbox on the provider's system." Brief on Rehearing En Banc for Senator Patrick J. Leahy as Amicus Curiae Supporting the United States and Urging Reversal, *United States v. Councilman*, No. 03-1383, 2004 WL 2707307, at *6 (1st Cir. Nov. 12, 2004). Before enacting the SCA, Congress had commissioned the Office of Technology Assessment to conduct a study (the "OTA Report") identifying the stages during which electronic communications would be most susceptible to unauthorized access. *See* U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties (1985) ("OTA Report") at 48. The OTA Report distinguished between "transmi[ssion]" of a communication "to the electronic mailbox," and "stor[age]" of the communication, with "storage" referring principally to storage in the mailbox maintained by the provider on the user's behalf, or storage in the provider's files for administrative purposes. This distinction was consistent with the testimony of industry representatives during hearings in 1985 immediately prior to the introduction of a bill "reflec[ting] the concerns" raised by those industry representatives—the bill which turned into ECPA. S. Rep. No. 99-541, at 4. The OTA Report was consistent with industry representatives' concerns that communications were particularly vulnerable while on the provider's servers, because hacking into such systems was perceived to be easier than acquiring a communication at points along the transmission path. *See Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks, Senate Comm. on the Judiciary*, 99th Cong. 1 (1987) at 121-22 (testimony of Philip M. Walker on behalf of the email industry). ECPA reflected Congress's intent to alleviate those concerns.

This legislative intent is effectuated in the majority of the cases construing the SCA. For example, in *Councilman*, after considering the SCA's legislative history, the First Circuit granted broad protection to stored electronic communications, acknowledging that "Congress sought to ensure that the messages and by-product files that are left behind after transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access." *United States v. Councilman*, 418 F.3d 67, 77 (1st Cir. 2005). Similarly, in *Theofel*, the Ninth Circuit found that the SCA "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility," analogizing to the way that the tort of trespass protects those who rent space from a commercial storage facility to store their sensitive documents. *Theofel*, 359 F.3d at 1072-73 (citations omitted).

Moreover, when enacting the SCA and ECPA, Congress intended to codify protections similar to the Fourth Amendment for communications stored by service providers. In 1986, long before the Sixth Circuit found in *Warshak* that users had a reasonable expectation of privacy in the contents of their emails, Congress feared that the Fourth Amendment did not provide adequate protection for communications hosted by third parties, such as email service providers (such as Gmail today). *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). For example, Congress was concerned that electronic communications would not be covered by the Fourth Amendment due to the judicially created third-party doctrine, which provides an exception to Fourth Amendment protection for information that is voluntarily shared with a third party. *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 444 (1976). Accordingly, Congress sought to codify Fourth Amendment-like protection for stored electronic communications and provide a minimum level of protection for these important new methods of communication. *See* S. Rep. No. 99-541, at 5

("[T]he law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens."); *see also* Christina Raquel, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud*, 55 SANTA CLARA L. REV. 467 (2015), citing Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes As Emails Get Dusty*, 88 B.U. L. REV. 1043, 1054 (2008) ("The Electronic Communications Privacy Act of 1986 ('ECPA') represents a Congressional endeavor to prevent the Fourth Amendment's third party doctrine from compromising the privacy interests of electronic communications stored by third parties.").

Moreover, in enacting the SCA, Congress intended to promote technological advancement by ensuring that users could be confident in the privacy of their stored electronic communications. Congress sought to provide a baseline of protection to "encourage the commercial use of 'innovative communications systems,' and discourage unauthorized users from obtaining access to communications to which they are not a party[.]" Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 41 (2015) (citing S. Rep. No. 99-541, at 5 (1986)). As the committee reports reflect, Congress was well aware of the need to protect against unauthorized access of a user's mailbox, both so that providers would not be deterred from offering new services, and potential customers would not be deterred from using them. *See*, *e.g.*, S. Rep. No. 99-541, at 5, reprinted in 1986 U.S.C.C.A.N. at 3559; H.R. Rep. No. 99-647, at 19.

II. The district court's ruling would have irrational and catastrophic consequences

A. Under the district court's narrow definition of "electronic storage," billions of communications would lose privacy protections

In the three decades since the enactment of the SCA, the use of, and dependence on, electronic communications has grown, and protecting these communications has become even more crucial.

Email is integral to our day-to-day interactions, and increasingly is the medium for a vast volume of private communications. Even two years ago, Gmail had over one billion monthly active users. This year, the number of email users worldwide is expected to exceed 3.8 billion, and the number of emails sent and received ***per day*** will exceed 281 billion. *Email Statistics Report, 2018-2022*, The Radicati Group (March 2018), https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf. We use email for every purpose—"[l]overs exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). As the U.S. Supreme Court has recognized, email and other forms of electronic communication are "essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010).

In addition, the SCA applies beyond email to myriad forms of electronic communication common to daily life in the twenty-first century, including text messages and social media messaging. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008) (text messages), *rev'd and remanded on other grounds* 560 U.S. 746 (2010); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010) (private communications through social media). The narrow definition of "electronic storage" proposed by the district court would eviscerate the protections afforded by the SCA and affect the vast number of people using these forms of electronic communication otherwise covered by the SCA. This case has widespread, real-world implications and will impact millions who communicate through email, text messaging, instant messaging, social media, and numerous other internet applications.

B. Under the district court's holding, the SCA would protect spam and unwanted communications, while protections for sensitive and intimate communications would be eviscerated

The district court's narrow interpretation of "electronic storage" would remove the most important private communications—messages that users have read and found important enough to keep—from the SCA's protections, while paradoxically, spam and unwanted communications would remain protected. Due to the widespread availability of free or low-cost electronic storage, email users in 2018 are likely to read and purposefully keep important emails, while also retaining unwanted and unread junk mail. Email services frequently offer vast storage space, such as Google's 15 gigabytes of free storage—the equivalent of about 150 yards of books on a shelf. Joel Lee, *Memory Sizes Explained—Gigabytes, Terabytes & Petabytes in Layman's Terms*, MakeUseOf.com (Aug. 14, 2012), https://www.makeuseof.com/tag/memory-sizes-gigabytes-terabytes-petabytes/. Email users can save, and typically find great utility in saving, their emails, whether read or unread. They can also employ tools to automatically sort their emails into separate inboxes or folders, such that users do not need to open unwanted emails to keep their inbox uncluttered. Accordingly, "the emails or private messages that are both the most important and the most private are the older messages that you have read through several times . . . . By contrast, the unopened emails in your inbox are likely to be commercial solicitations." *Electronic Communications Privacy Act and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the Comm. on the Judiciary*, 111th Cong. 2, at 123 (2010) (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP).

The district court's decision would lead to an absurd result, leaving unprotected a recipient's most intimate and important emails while retaining protection for a recipient's ignored and neglected emails. When email users open messages from colleagues, friends, families, or even from their banks or doctors, these private communications would lose protection under the district court's interpretation of the SCA. In contrast, junk mail or spam—at best, commercial promotions an email user opted into and at worst, unsolicited scams—would retain protection as they linger unopened and unwanted in a user's email account. This irrational outcome would undermine the goals of the SCA, further suggesting that the district court incorrectly interpreted the meaning of "electronic storage."

C. The district court's holding would have broad implications for both civil and criminal cases, allowing third parties and the government access to users' digital communications once they are read

The definition of "electronic storage" at issue in this case applies to both the civil ***and*** criminal provisions of ECPA, and could have a widespread impact beyond the narrow facts of this case. In addition to creating civil causes of action, such as holding private actors liable for accessing stored communications without authorization, the SCA restricts the government's ability to obtain user data from service providers without a warrant. As discussed *supra*, Section I.D, Congress enacted ECPA and the SCA in part out of concern that electronic communications such as emails would not be covered by the Fourth Amendment while stored by a service provider due to the third-party doctrine (which provides an exception to the Fourth Amendment when information is voluntarily shared with a third party). That is, Congress feared that the government could sidestep the Fourth Amendment by simply requesting users' emails directly from the email service provider (without a warrant), rather than obtaining emails from the users themselves. To prevent this, ECPA extended Fourth Amendment-like protections to communications held by these third-party service providers to provide a baseline of protection to electronic communications.

In 2008, the Sixth Circuit in *Warshak* ruled that the Fourth Amendment's "reasonable expectation of privacy" standard applies to the contents of emails. *Warshak*, 631 F.3d 266, 286 n.12; *see also United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (finding a reasonable expectation of privacy in email content); *see also In re Applications for Search Warrants for Info. Associated with Target Email Address*, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (same). Based on *Warshak*'s ruling, the Department of Justice has voluntarily adopted the policy of seeking a warrant whenever it requests the contents of an email. *See* H.R. Rep. No. 114-528, at 9 (Apr. 26, 2016). Still, statistics from Google's Transparency Report show that, in 2017 alone, the U.S. government sent more than 32,000 requests for user data to Google, including requests under ECPA and the SCA, with more than 80% of those requests leading to the production of at least some user data. *Google Transparency Report*, https://transparencyreport.google.com/user-data/overview (last visited May 28, 2018). Similarly, Facebook's Transparency Report shows that the U.S. government sent more than 65,000 requests for user data to Facebook in 2017, including requests under ECPA and the SCA, with 85% of those requests leading to the production of at least some user data. *Facebook Transparency Report*, https://transparency.facebook.com/government-data-requests/country/US (last visited May 28, 2018). Although several circuit courts have extended Fourth Amendment protections to emails held by third-party service providers, the SCA additionally codifies Fourth Amendment-like protections for these stored communications. *See, e.g.*, *Warshak*, 631 F.3d 266. Thus, at the boundaries of Fourth Amendment protection, the SCA still plays a crucial role in affording internet users a baseline of privacy protection, and the district court's narrow definition of "electronic storage" could have sweeping implications for the government's ability to obtain data from service providers.

In the civil context, where the Fourth Amendment does not apply, the SCA provides vital protections from unauthorized access of users' communications. These protections are more important than ever in today's cybersecurity landscape, and the district court's narrow definition of "electronic storage" could devastate the ability of users to seek redress when their privacy is violated. While the unauthorized access of user data is not a new problem, large-scale data breaches have increased in frequency as more data is stored online and new exploits are found by cybercriminals. *See* Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, Wired Magazine (Apr. 17, 2015), https://www.wired.com/2015/04/therealdeal-zero-day-exploits/. The SCA provides users with recourse for cyberattacks involving stored communications, creating affirmative causes of action that extend beyond the Constitution to hold private actors liable. Limiting the scope of the SCA by taking a narrow view of "electronic storage," as the district court has done in *Hately*, would leave many internet users without recourse under the SCA when their sensitive data is accessed without authorization.[5]

D. The district court's narrow definition of "backup protection" is based on an antiquated understanding of email technology

In holding that "backups" refers only to transitory copies "created and stored separate and apart from the copies maintained to facilitate continuing access by the user through his account," the district court draws a false distinction between "backup storage copies" and a "service copy maintained to be available to the user."

[5] While there would be no SCA liability, there could still be recourse under the Computer Fraud and Abuse Act, which imposes liability for unauthorized access to a "protected computer" (including any computer connected to the internet), regardless of whether the data obtained thereby was "in electronic storage" under ECPA. *See* 18 U.S.C. § 1030(a).

Hately, slip op. at 9 (E.D. Va. Mar. 14, 2018). That false distinction cannot be squared with the way that modern electronic communications services operate. Contrary to the district court's premise, there ***is no distinction*** between "service copies" and "backup storage copies" in today's cloud-based email systems. *Id.* The district court's attempt to draw a distinction where none exists demonstrates the fundamental error in its holding that an electronic communication is no longer "in electronic storage" once opened.

Increasingly, emails and other electronic communications are stored on cloud-based, redundant email systems, rather than directly on users' phones or computers. Cloud-based technologies give consumers the ability to access all of their information on all of their devices. *ECPA Part 1: Lawful Access to Stored Content: Hearing Before the H. Judiciary Subcomm. on Crime, Terrorism, Homeland Sec. and Investigations*, 113th Cong. 1 (2013) (written testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.) ("Everyday processes and information that are typically run and stored on local computers—such as email, documents, and calendars—can now be accessed securely anytime, anywhere, and with any device through an Internet connection."). In a cloud-based email system, ***all*** emails are stored on the service provider's servers—including the "copies maintained to facilitate continuing access by the user through his account." The user views a duplicate copy of the email stored in the service provider's servers, rather than receiving the one and only copy of the email. There is no significant status change of the message when a user first views the email—that is, "the act of 'reading' the email is of no legal moment, because it does not transform the storage from 'temporary' to permanent. Nor does the user's action or inaction have any impact on the physical location of the email—it remains on the provider's servers and is not downloaded to [the user's] computer." *Id.*

The district court's narrow definition would apply only when a single specific email is downloaded to a ***single*** device such as a computer. Older email protocols, such as the Post Office Protocol (POP3), functioned in this manner. The POP3 protocol allowed email access on a single device by downloading all new messages to that device. When a user connected to the internet and updated his or her inbox, ***one*** copy was downloaded to his or her personal computer. In contrast, emails for a recipient using newer protocols like IMAP or webmail are stored on servers—not an individual's device. *Id.* ("Today, . . . webmail is the predominant form of personal email communication and webmail is seldom delivered to a user for local storage on his or her own PC. Rather, it stays in the cloud and the user interacts with the mail on the provider's servers."). In other words, there is no ***single copy*** of the email that is delivered to the mail client on the recipient's computer or phone. Instead, a copy of the email is accessible, viewable, modifiable, and deletable on ***all*** of the user's devices.

Many email service providers also utilize completely redundant systems consisting of multiple data servers to decrease email downtime (*i.e.*, users being unable to access their email) or loss of information due to component failure. *Reliability: How Can Google Be So Reliable?*, Google Cloud Help, https://support.google.com/googlecloud/answer/6056635 ("All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation."). This type of system allows service providers to build systems with nearly zero loss of information using inexpensive hardware. *See id*. In redundant systems, a single email is stored on multiple servers, likely in different locations around the country, and possibly around the world. Each server will have a different "copy" of the same email. In other words, every copy can be considered a "backup" in modern configurations, and each piece of data can be accessed through multiple pathways. *See* Robert J. Shimonski, *The Importance of Network Redundancy*, TechGenix (June 15, 2010), http://techgenix.com/importance-network-redundancy/. Thus, the district court erred in drawing a distinction between "backup copies" and "service copies" in interpreting "electronic storage."

E. If the district court's holding is affirmed, stored communications will be subject to different privacy protections in different states

If the district court's holding is affirmed, the narrow definition of "electronic storage" will significantly reduce the protections offered by the SCA within the

Fourth Circuit. Residents of the Fourth Circuit will be prejudiced by such a ruling—they stand to lose SCA protections for their private and sensitive communications, once opened. If the district court's ruling is upheld, private communications in the Fourth Circuit would not have the same standard of protection as communications in other jurisdictions, leading to counterintuitive results. If an employee sends confidential business information to her colleagues in the Fourth Circuit and the Ninth Circuit, and that communication is accessed without authorization, her Fourth Circuit colleagues would not be able to bring the same lawsuit as their Ninth Circuit coworkers. This result is also inconsistent with how people actually use electronic communication systems such as email, social media, and instant messaging. Electronic communication systems facilitate communications across state lines—and a single data breach often affects people across the country. In such a scenario, the district court's narrow construction of "electronic storage" would severely limit the ability of Fourth Circuit residents to seek redress under the SCA.

III. These irrational and catastrophic consequences cannot be squared with Congress's intent in passing ECPA and the SCA

As discussed *supra*, Section I.D, Congress had numerous forward-thinking policy goals in enacting ECPA and the SCA, which are undermined by the district court's holding in this case. Retaining privacy protections for only the unwanted messages that are ignored by users, while removing those vital protections for the very communications that are important enough for users to open is absurd and clearly contrary to Congress's intent. Furthermore, Congress enacted the SCA to encourage the commercial use of innovative communications systems, but the district court's erroneous interpretation of "electronic storage" is irreconcilable with modern cloud-based communication systems. The district court's decision has widespread implications for the billions of electronic communications sent each day, and would jeopardize the privacy of countless important, sensitive communications. It should be overturned.

CONCLUSION

For these reasons, this Court should reverse the district court's summary judgment that, because they had been opened, the emails at issue in this case were not "in electronic storage" for the purposes of the SCA.

Dated: May 29, 2018

Respectfully submitted,

/s/ Marta F. Belcher
Marta F. Belcher (*counsel of record*)
James R. Batchelder
Monica A. Ortel
James H. Rickard
ROPES & GRAY LLP
1900 University Avenue, 6th Floor
East Palo Alto, CA 94303
(650) 617-4000

Evan Gourvitz
Lance W. Shapiro
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036
(212) 596-9000

Kathryn C. Thornton
ROPES & GRAY LLP
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
(202) 508-4600

Gregory T. Nojeim
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street NW, Suite 200
Washington, D.C. 20005
(202) 637-9800

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

Kevin Bankston
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE
740 15th Street NW, Suite 900
Washington, D.C. 20036
(202) 986-2700

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on this 29th day of May, 2018, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit using the appellate CM/ECF system.

Counsel for all parties to the case are registered CM/ECF users and will be served by the appellate CM/ECF system.

/s/ Marta F. Belcher

Marta F. Belcher
ROPES & GRAY LLP
1900 University Avenue, 6th Floor
East Palo Alto, CA 94303
(650) 617-4000

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(G), I hereby certify that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 29(a)(5).

1. In compliance with Federal Rules of Appellate Procedure 32(a)(5) and 32(a)(6), the brief has been prepared in proportionally spaced Times New Roman Font with 14-point type using Microsoft Word 2016.

2. Exclusive of the exempted portions of the brief, as provided in Federal Rule of Appellate Procedure 32(f), the brief contains 5,303 words, consistent with Federal Rule of Appellate Procedure 29(a)(5). As permitted by Federal Rule of Appellate Procedure 32(g)(1), I have relied upon the word count feature of Microsoft Word 2016 in preparing this certificate.

Dated: May 29, 2018

/s/ Marta F. Belcher

Marta F. Belcher
ROPES & GRAY LLP
1900 University Avenue, 6th Floor
East Palo Alto, CA 94303
(650) 617-4000

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 18-1306 as

☐ Retained ☐ Court-appointed(CJA) ☐ Court-assigned(non-CJA) ☐ Federal Defender ☑ Pro Bono ☐ Government

COUNSEL FOR: The Center for Democracy & Technology, The Electronic Frontier Foundation,

and New America's Open Technology Institute as the

(party name)

☐ appellant(s) ☐ appellee(s) ☐ petitioner(s) ☐ respondent(s) ☑ amicus curiae ☐ intervenor(s) ☐ movant(s)

/s/ Marta F. Belcher
(signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's Manage My Account.

Marta F. Belcher
Name (printed or typed)

(650) 617-4000
Voice Phone

ROPES & GRAY LLP
Firm Name (if applicable)

(650) 617-4090
Fax Number

1900 University Ave., 6th Floor
East Palo Alto, CA 94303
Address

Marta.Belcher@ropesgray.com
E-mail address (print or type)

CERTIFICATE OF SERVICE

I certify that on May 29, 2018 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Marta F. Belcher
Signature

5/29/2018
Date