UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

SECURITIES AND EXCHANGE, COMMISSION, *Plaintiff*, *v.*	)	Civil Action No. 8:15cv1339-GJH
NORTH STAR FINANCE, LLC, ET AL. *Defendants*,	)	
and	)	
GOODWILL FUNDING INC. and CHAREL WINSTON, *Relief Defendants.*	)	

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF NON-PARTY YAHOO! INC.'S OPPOSITION TO COMMISSION'S APPLICATION FOR AN ORDER REQUIRING COMPLIANCE WITH ADMINISTRATIVE SUBPOENA

Mark Rumold*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
mark@eff.org

**Pro hac vice* pending

Jan Berlage
GOHN HANKEY STICHEL & BERLAGE LLP
201 N. Charles Street, Suite 2101
Baltimore, MD 21201
Telephone: (410) 752-1261
Facsimile: (410) 752-2519
JBerlage@ghsllp.com

Of counsel:
Joseph Dudek
GOHN HANKEY STICHEL & BERLAGE LLP
201 N. Charles Street, Suite 2101
Baltimore, MD 21201
Telephone: (410) 752-0892
Facsimile: (410) 752-2519
JDudek@ghsllp.com
Licensed to practice in the State of New York

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iii

INTRODUCTION 1

I. INTERNET USERS HAVE A REASONABLE EXPCETATION OF PRIVACY IN EMAILS STORED WITH A THIRD-PARTY PROVIDER 2

II. THE GOVERNMENT MUST OBTAIN A WARRANT TO COMPEL DISCLOSURE OF PRIVATE EMAILS STORED WITH A THIRD-PARTY PROVIDER. 3

III. OTHER MECHANISMS EXIST TO OBTAIN THE INFORMATION THE SEC SEEKS WITHOUT INTRUDING ON A USER'S REASONABLE EXPECTATION OF PRIVACY. 6

CONCLUSION 8

CERTIFICATE OF SERVICE 9

TABLE OF AUTHORITIES

Federal Cases

Boyd v. United States,
116 U.S. 616 (1886) ... 2

City of Los Angeles v. Patel,
135 S. Ct. 2443 (2015) ... 5

Coolidge v. New Hampshire,
403 U.S. 443 (1971) ... 6

Donovan v. Lone Steer,
464 U.S. 408 (1984) ... 5

In re Applications for Search Warrants for Information Associated with Target Email Address,
No. 12–MJ–8119–DJW, 2012 WL 4383917 (D. Kan. Sept. 21, 2012) ... 2

In re Grand Jury Subpoena (Kitzhaber),
828 F.3d 1083 (9th Cir. 2016) ... 2

In re Subpoena Duces Tecum (Bailey),
228 F.3d 341 (4th Cir. 2000) ... 5

In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation ("*Microsoft Ireland*"),
829 F.3d 197 (2d Cir. 2016) ... 3

Jones v. United States,
357 U.S. 493 (1958) ... 3

Katz v. United States,
389 U.S. 347 (1967) ... 3, 4

Oklahoma Press Publishing Co. v. Walling,
327 U.S. 186 (1946) ... 4

Penfield Co. v. SEC,
330 U.S. 585 (1947) ... 5

Riley v. California,
134 S. Ct. 2473 (2014) ... 2, 4, 6, 7

See v. City of Seattle,
387 U.S. 541 (1967) ... 5

United States v. Bynum,
604 F.3d 161 (4th Cir. 2010) 6

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 2

United States v. Jacobsen,
466 U.S. 109 (1984).. 5

United States v. Lucas,
640 F.3d 168 (6th Cir. 2011) 2

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

United States v. Morton Salt Co.,
338 U.S. 632 (1950).. 4

United States v. United States District Court for the Eastern District of Michigan (Keith),
407 U.S. 297 (1972).. 4, 6

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 2, 3, 5

Zurcher v. Stanford Daily,
436 U.S. 547 (1978).. 6

Constitutional Provisions

U.S. Const. amend. IV 2, 3, 4, 6

INTRODUCTION

At issue in the above-captioned matter is a question of extraordinary significance to the privacy of American Internet users: may the government compel a third-party service provider to disclose the private emails of its users, without first obtaining a warrant or the consent of the user?

It may not.

Amici the Electronic Frontier Foundation ("EFF") and the Center for Democracy and Technology ("CDT") urge the Court to reject the SEC's attempt to obtain email content from Yahoo with an administrative subpoena.[1] Consistent with longstanding and widely accepted precedent of the Sixth Circuit and other courts, as well as relevant precedent of the Supreme Court, the government may only compel the disclosure of private email from a third-party service provider with a warrant based upon probable cause.

---

[1] EFF is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF served as amicus curiae in the leading case on the question at issue here, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

CDT is a nonprofit public interest organization working to ensure that the human rights we enjoy in the physical world are realized online, and that technology serves as an empowering force for people worldwide. Integral to this work is CDT's representation of the public interest in the creation of an open, innovative, and decentralized Internet that promotes the constitutional and democratic values of free expression, privacy, and individual liberty. Of particular interest here, CDT leads a coalition of advocacy organizations, academics, trade associations and companies with the goal of modernizing the Electronic Communications Privacy Act.

No party or party's counsel participated in the writing of the brief in whole or in part. No party, party's counsel, or other person contributed money to fund the preparation or submission of the brief. Amici are neither sponsored by, nor in any way affiliated with, any of the parties or non-parties to this case.

I. INTERNET USERS HAVE A REASONABLE EXPCETATION OF PRIVACY IN EMAILS STORED WITH A THIRD-PARTY PROVIDER

All parties agree on at least one point: Internet users have a reasonable expectation of privacy in the content of private emails stored with a third-party provider. *See* Opposition at 12-15 (ECF No. 291); Reply at 2 (ECF No. 295).

"The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities." *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc). These "digital papers"—which include emails stored with third-party providers—"implicate[] the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers[.]'" *Id.* at 964. This right "reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government. These records are expected to be kept private and this expectation is one that society is prepared to recognize as 'reasonable.'" *Id*. (citations and quotations omitted). As the Supreme Court recently recognized, digitally stored information, including email, contains "the privacies of life." *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

Emails stored with a third party thus receive the full panoply of the Fourth Amendment's protections. The Sixth and Ninth Circuits, in addition to other courts, have recognized this commonsense conclusion. *See United States v. Warshak*, 631 F.3d 266, 285-88 (6th Cir. 2010); *In re Grand Jury Subpoena (Kitzhaber)*, 828 F.3d 1083, 1090-91 (9th Cir. 2016); *see also United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011); *In re Applications for Search Warrants for Information Associated with Target Email Address*, No. 12–MJ–8119–DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012).

SEC has offered no reason—and none exists—for the Court to deviate from this

established precedent.

II. THE GOVERNMENT MUST OBTAIN A WARRANT TO COMPEL DISCLOSURE OF PRIVATE EMAILS STORED WITH A THIRD-PARTY PROVIDER.

Because users have a reasonable expectation of privacy in their email, the Fourth Amendment requires the government to obtain a warrant before it can compel a third party to disclose it.

The Fourth Amendment prohibits unreasonable searches and seizures. U.S. Const. amend. IV. A "search," for purposes of the Fourth Amendment, occurs when the government intrudes upon an individual's reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). Searches carried out without a warrant are "per se unreasonable"—and thus prohibited—unless one of the "specifically established and well-delineated exceptions" to the warrant requirement applies. *Id*. at 357; *see also Warshak*, 631 F.3d at 288 (government violated Fourth Amendment by obtaining contents of emails without a warrant).

Here, SEC recognizes and concedes that Yahoo's user has a reasonable expectation of privacy in the content of his emails. *See* Reply at 2 (ECF No. 295). There can also be no dispute that the administrative subpoena it issued to Yahoo is not a warrant. *See In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* ("*Microsoft Ireland*"), 829 F.3d 197, 214 & n.24 (2d Cir. 2016). Nor does SEC point to one of the "jealously and carefully drawn" exceptions to the warrant requirement to justify its intrusion. *Jones v. United States*, 357 U.S. 493, 499 (1958).

To resolve this Motion, then, the Court need not proceed further: compelled intrusion into the reasonable expectation of privacy of Yahoo's user is prohibited absent a warrant or some exception to the warrant requirement. *Warshak*, 631 F.3d at 288; *see also Microsoft Ireland*, 829

F.3d at 214 ("When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions").

SEC argues that requiring a warrant would "undermine the Commission's law enforcement mission." Reply at 18. But "the warrant requirement is an 'important working part of our machinery of government,' not merely an 'inconvenience to be somehow "weighed" against'" the government's interest in pursuing its objectives or acting efficiently. *Riley v. California*, 134 S. Ct. 2473, 2493 (2014) (citations omitted). Indeed, even in matters as weighty as domestic national security investigations, the Supreme Court has rejected warrantless intrusions into areas in which a person has a reasonable expectation of privacy. *See United States v. United States District Court for the Eastern District of Michigan (Keith)*, 407 U.S. 297, 313 (1972).

Rather than obtain a warrant (or rely on a valid exception, like consent), SEC instead claims that an administrative subpoena, coupled with the opportunity to initiate an adversarial judicial process, satisfies the Fourth Amendment's requirements. In support of this position, SEC primarily relies on *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946), and its progeny, cases that predate the *Katz* "reasonable expectation of privacy" test by many years.

SEC's reliance on *Oklahoma Press* is misplaced. That case, by its own terms, "present[ed] no question of actual search and seizure." 327 U.S. at 195; *accord United States v. Morton Salt Co.*, 338 U.S. 632, 651-53 (1950) (noting disclosures compelled by subpoena "shall not be unreasonable"). SEC thus erroneously claims that its subpoena does not constitute a search. Reply at 15. Since *Katz*, a search under the Fourth Amendment has been defined precisely in terms of an intrusion into a reasonable expectation of privacy. *United States v.*

Jacobsen, 466 U.S. 109, 113 (1984). As described above, the compelled disclosure of email to the government—and the attendant intrusion into a user's reasonable expectation of privacy—*does* constitute a search and is therefore unreasonable unless undertaken with a warrant.

Ultimately, none of the cases cited by SEC stand for the proposition that the government may use an administrative subpoena to compel production, access to, or otherwise intrude on an area protected by an individual's reasonable expectation of privacy, absent some exception to the warrant requirement. *See, e.g.*, *Penfield Co. v. SEC*, 330 U.S. 585, 591 (1947) (subpoena may be challenged if it results in an "unreasonable search and seizure") (Frankfurter, J., dissenting); *See v. City of Seattle*, 387 U.S. 541, 545 (1967) ("[A]dministrative entry, without consent, upon the portions of commercial premises which are not open to the public may only be compelled through. . . the framework of a warrant procedure[.]"); *Donovan v. Lone Steer*, 464 U.S. 408, 413 (1984) (subpoena did not "authorize either entry or inspection of appellee's premises").

In particular, SEC's reliance on *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), and *In re Subpoena Duces Tecum (Bailey)*, 228 F.3d 341 (4th Cir. 2000), is misplaced. Both cases involved warrantless access to the records of an individual or entity *from* the individual or entity subject to the regulation. *Patel*, 135 S. Ct. at 2447 (motel operators' records); *Bailey*, 228 F.3d at 344 (physician's record). Neither case suggests that the government may obtain from a third party what it cannot obtain directly from the target of its investigation.

Indeed, the cases that do uphold government subpoenas for records held by third parties rely on the proposition that providing these records to a third party extinguishes a reasonable expectation of privacy in the records. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Bailey*, 228 F.3d at 351 (noting patients' "reduced expectation of privacy" in physician records). But in *Warshak*, the Sixth Circuit explicitly rejected the application of the so-called "third-party

doctrine" to a subpoena for the content of stored emails. 631 F.3d at 288; *see also United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (rejecting challenge to FBI subpoena for "internet and phone 'subscriber information'" because the government "did not invade any legitimate privacy interest").

Further, the SEC's attempts to rehabilitate its subpoena as *more* protective of a user's privacy than a warrant should be rejected. The warrant clause's dual requirements of probable cause and particularity directly prohibit "baseless searches." *Keith*, 407 U.S. at 316 (1972). These requirements ensure that the searches that do occur are "as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Subpoenas, in contrast, sweep more broadly, do not require the review and approval of a neutral magistrate, and require a lower factual showing. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 562-63 (1978). Even notice and the opportunity to contest the subpoena do not cure the Fourth Amendment defects that exist.

III. OTHER MECHANISMS EXIST TO OBTAIN THE INFORMATION THE SEC SEEKS WITHOUT INTRUDING ON A USER'S REASONABLE EXPECTATION OF PRIVACY.

The privacy interests of users and the related constitutional requirements appropriately force agencies like the SEC to pursue paths of investigation in civil cases *other than* compelling third-party service providers to disclose emails. While going directly to a third-party service provider may be attractive in a civil investigation "in the interest of efficiency," SEC Motion at 4, investigative efficiency is not a consideration that overrides constitutional safeguards. *Riley v. California*, 134 S. Ct. at 2493 (citations omitted)

As Yahoo has explained, *see* Opposition at 23-26, the SEC has a number of options at its disposal to obtain the information it seeks in civil investigations without infringing on users' Fourth Amendment rights.

First, SEC can obtain the information from users themselves, either through their own

production of emails or from service providers after obtaining their consent to disclosure. If a user refuses to produce emails or withholds their consent, as here, SEC can take steps, just as any civil litigant, to compel compliance with its requests. Such compulsion—which may include monetary sanctions, adverse evidentiary inferences, or other litigation sanctions—will likely result in either the production of information the SEC seeks or a proportionate litigation consequence. Second, SEC can take steps to obtain the same emails with the consent of another party. Third, SEC can substitute the information it seeks with a subpoena for information that is not protected by the users' reasonable expectation of privacy.

Barring that, in a case that includes a criminal investigation, as here,[2] the SEC, with the assistance of the Department of Justice, can resort to a tried-and-true method—"get[ting] a warrant." *Riley*, 134 S. Ct. at 2495.

[2] *See* https://www.sec.gov/litigation/litreleases/2015/lr23262.htm (noting the FBI arrested Martin on wire fraud charges).

CONCLUSION

The Court should deny SEC's motion to compel compliance with its administrative subpoena.

June 16, 17

Respectfully submitted,

By: /s/ *Jan Berlage*
Jan Berlage

Jan Berlage (No. 23937)
GOHN HANKEY STICHEL & BERLAGE LLP
201 N. Charles Street, Suite 2101
Baltimore, Maryland 21201

Mark Rumold
pro hac vice admission pending
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109

Joseph Dudek
GOHN HANKEY STICHEL & BERLAGE LLP
of counsel
201 N. Charles Street, Suite 2101
Baltimore, Maryland 21201

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on June 16, 17, I caused the foregoing to be served by electronic mail on counsel for the defendants, relief defendants, and non-party at the following addresses:

Counsel for North Star Finance, Ellis, and Oda

Jacob S. Frenkel
jfrenkel@dickenson-wright.com

Alexander C. Vincent
avincent@shulmanrogers.com

Counsel for Non-party Yahoo! Inc.

Jeffrey Landis
jeff@zwillgen.com

Marc Zwillinger
marc@zwillgen.com

Counsel for Securities Exchange Commission

Jeffrey Berger
BergerJe@sec.gov

Pro Se Defendants and relief defendants

Tom Ellis
tomconfidential@gmail.com

Yasuo Oda
yasuoconfidential@gmail.com

Michael K. Martin /
Capital Source Lending LLC
capitalsourcelending@yahoo.com

Sharon L. Salinas /
Capital Source Funding LLC
leglzwlf@gmail.com

Thomas H. Vetter
tom.vetter2@gmail.com

Goodwill Funding Inc.
Cwinston2000@aol.com

Charel Winston
Cwinston2000@aol.com

/s/ *Jan Berlage*
Jan Berlage