

# 14-2985-cv

---

---

IN THE  
**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 OF *AMICI CURIAE* MEDIA ORGANIZATIONS  
IN SUPPORT OF APPELLANT**

---

LAURA R. HANDMAN  
ALISON SCHARY  
DAVIS WRIGHT TREMAINE LLP  
1919 Pennsylvania Avenue NW,  
Suite 800  
Washington, DC 20006  
(202) 973-4200

*Attorneys for Amici Curiae  
Media Organizations*

---

---

OF COUNSEL

Indira Satyendra  
John W. Zucker  
ABC, INC.  
77 West 66th Street, 15th Floor  
New York, NY 10036  
*Counsel for ABC, Inc.*

Richard A. Bernstein  
SABIN, BERMANT & GOULD LLP  
One World Trade Center  
44th Floor  
New York, NY 10007  
*Counsel for Advance Publications,  
Inc.*

Kevin M. Goldberg  
FLETCHER HEALD & HILDRETH  
1300 North 17th Street, 11th Floor  
Arlington, VA 22209  
*Counsel for the American  
Society of News Editors and the  
Association of Alternative  
Newsmedia*

Scott Searl  
BH MEDIA GROUP  
1314 Douglas St.  
Suite 1500  
Omaha, NE 68102  
*Counsel for BH Media Group*

David Vigilante  
CABLE NEWS NETWORK, INC.  
One CNN Center  
Atlanta, GA 30303  
*Counsel for Cable News Network,  
Inc.*

Andrew Goldberg  
THE DAILY BEAST  
555 West 18th Street  
New York, New York 10011  
*Counsel for The Daily Beast  
Company LLC*

Matthew Leish  
Cyna Alderman  
NEW YORK DAILY NEWS  
4 New York Plaza  
New York, NY 10004  
*Counsel for Daily News, L.P.*

David M. Giles  
THE E.W. SCRIPPS COMPANY  
312 Walnut St., Suite 2800  
Cincinnati, OH 45202  
*Counsel for The E.W. Scripps  
Company*

Lynn Oberlander  
FIRST LOOK MEDIA, INC.  
162 Fifth Avenue, 8th Floor  
New York, NY 10010  
*Counsel for First Look Media, Inc.*

Jessica Bohrer  
FORBES MEDIA  
60 Fifth Avenue  
New York, NY 10011  
*Counsel for Forbes Media*

Dianne Brandi  
FOX NEWS NETWORK LLC  
1211 Avenue of the Americas  
Second Floor  
New York, NY 10036-8795  
*Counsel for Fox News Network LLC*

Barbara W. Wall  
GANNETT CO., INC.  
7950 Jones Branch Drive  
McLean, VA 22107  
*Counsel for Gannett Co., Inc.*

Gillian Phillips  
GUARDIAN NEWS & MEDIA  
Kings Place  
90 York Way  
London N1 9GU  
England  
*Counsel for Guardian News & Media*

Eve Burton  
Jonathan Donnellan  
Kristina Findikyan  
HEARST CORPORATION  
300 West 57th Street, 40th Floor  
New York, NY 10019  
*Counsel for Hearst Corporation*

Karole Morgan-Prager  
Juan Cornejo  
THE McCLATCHY COMPANY  
2100 Q Street  
Sacramento, CA 95816  
*Counsel for The McClatchy Company*

James Cregan  
Mary Holland  
MPA – THE ASSOCIATION OF  
MAGAZINE MEDIA  
1211 Connecticut Avenue  
NW, Suite 610  
Washington, DC 20036  
*Counsel for MPA – The Association  
of Magazine Media*

Charles D. Tobin  
HOLLAND & KNIGHT LLP  
800 17th Street NW, Suite 1100  
Washington, DC 20006  
*Counsel for the National Press Club*

Mickey H. Osterreicher  
NATIONAL PRESS PHOTOGRAPHERS  
ASSOCIATION  
1100 M&T Center  
3 Fountain Plaza  
Buffalo, NY 14203  
*Counsel for National Press  
Photographers Association*

Jonathan D. Hart  
Ashley Messenger  
NATIONAL PUBLIC RADIO, INC.  
1111 North Capitol Street, NE  
Washington, DC 20002  
*Counsel for National Public Radio,  
Inc.*

Kurt A. Wimmer  
COVINGTON & BURLING LLP  
850 10th Street, NW  
Washington, DC 20001  
*Counsel for Newspaper Association of  
America*

Michael Kovaka  
COOLEY LLP  
1299 Pennsylvania Avenue, NW  
Suite 700  
Washington, DC 20004  
*Counsel for Online News Association*

Katherine G. Bass  
PEN AMERICAN CENTER, INC.  
588 Broadway, Suite 303  
New York, NY 10012  
*Counsel for PEN American Center,  
Inc.*

Bruce Brown  
Gregg P. Leslie  
THE REPORTERS COMMITTEE  
FOR FREEDOM OF THE PRESS  
1101 Wilson Boulevard  
Suite 1100  
Arlington, VA 22209  
*Counsel for The Reporters Committee  
for Freedom of the Press*

Julie Xanders  
Jeffrey Glasser  
TRIBUNE PUBLISHING COMPANY,  
INC.  
202 West 1st Street  
Los Angeles, CA 90012

Karen H. Flax  
TRIBUNE PUBLISHING COMPANY,  
INC.  
435 North Michigan Avenue  
Chicago, IL 60611  
*Counsel for Tribune Publishing  
Company, Inc.*

Christoph Fiedler  
VERBAND DEUTSCHER  
ZEITSCHRIFTENVERLEGER (VDZ)  
Markgrafenstraße 15, D-10969  
Berlin, Germany  
*Counsel for Verband Deutscher  
Zeitschriftenverleger (VDZ), the  
German Magazine Publishers  
Association*

James A. McLaughlin  
John B. Kennedy  
THE WASHINGTON POST  
1150 15th St., NW  
Washington, DC 20071  
*Counsel for The Washington Post*

## CORPORATE DISCLOSURE STATEMENTS

Pursuant to Rules 26.1 and 29(c)(1) of the Federal Rules of Appellate Procedure, undersigned counsel for *amici curiae* provide the following disclosures of corporate identity:

**ABC, Inc.** is an indirect, wholly-owned subsidiary of The Walt Disney Company, which is publicly held.

**Advance Publications, Inc.** has no parent corporation, and no publicly held corporation owns 10 percent or more of its stock.

The **American Society of News Editors** is a private, non-stock corporation that has no parent.

The **Association of Alternative Newsmedia** has no parent corporation and does not issue any stock.

**BH Media Group, Inc.** is a Delaware corporation whose direct parent company is Berkshire Hathaway Credit Corporation, which is a subsidiary of Berkshire Hathaway Inc., a publicly traded company (NYSE: BRK.A and BRK.B). BH Media Group also operates and manages WPLG-TV, the ABC affiliated station in Miami, which is owned by National Indemnity Company, which is also a subsidiary of BH Media Group, Inc.

**Cable News Network, Inc.** is a wholly owned subsidiary of Turner Broadcasting System, Inc., which itself is a wholly owned subsidiary of Time Warner Inc., a publicly traded corporation.

The parents of **The Daily Beast Company LLC** are TDB Holdings, Inc. and the Sidney Harman Trust. TDB Holdings, Inc. is a subsidiary of IAC/InterActiveCorp, a publicly traded company. IAC holds a controlling interest in The Daily Beast.

**Daily News, L.P.** is a limited partnership, the general partner of which is New DN Company, a privately held corporation. No publicly held corporation holds an interest of 10 percent or more in Daily News, L.P.

The **European Publishers Council** has no parent company and no publicly held company owns 10 percent or more of its shares.

**The E.W. Scripps Company** is a publicly traded corporation. It has no parent corporation, and no publicly owned company owns 10 percent or more of its stock.

**First Look Media, Inc.** is a non-stock corporation organized under the laws of Delaware. No publicly held corporation holds an interest of 10 percent or more in First Look Media, Inc.

**Fox News Network LLC**, a private non-governmental non-party, hereby certifies that it is wholly owned by Fox Television Stations, Inc., which, in turn, is wholly owned by Twenty-First Century Fox, Inc. Twenty-First Century Fox, Inc. is the ultimate corporate parent of Fox News and is a publicly traded corporation.

**Forbes, Inc.** states that the parent of company of Forbes, Inc. is Forbes Family Holdings Inc., that the parent company of Forbes Family Holdings Inc. is SBKTM Holdings Inc., and that no publicly held corporation owns 10 percent or more of the stock of Forbes, Inc.

**Gannett Co., Inc.** is a publicly traded company and has no affiliates or subsidiaries that are publicly owned. No publicly held company holds 10 percent or more of its stock.

**Guardian News & Media Limited** discloses that its parent company is Guardian Media Group, PLC. No publicly held company owns 10 percent or more of Guardian News & Media's stock.

**Hearst Corporation** is a diversified, privately held company. No publicly held company owns 10 percent or more of its stock.

**The McClatchy Company** is a publicly owned corporation. No publicly held company owns 10 percent or more of its stock.



**MPA - the Association of Magazine Media** has no parent corporation, and no publicly held corporation owns 10 percent or more of its stock.

The **National Press Club** is a not-for-profit corporation that has no parent company and issues no stock.

The **National Press Photographers Association** is a 501(c)(6) nonprofit organization that has no parent company and issues no stock.

**National Public Radio, Inc.** is a privately supported, not-for-profit membership organization that has no parent company and issues no stock.

The **Newspaper Association of America** is a non-stock corporation with no parent corporation, and no publicly held corporation owns 10 percent or more of any form of interest in it.

The **Online News Association** is a nonprofit organization. It has no parent company and issues no stock.

**PEN American Center, Inc.** is a nonprofit organization. It has no parent company and issues no stock.

The **Reporters Committee for Freedom of the Press** is an unincorporated association of reporters and editors with no parent corporation and no stock.

Blethen Corporation owns a majority of the voting stock of **Seattle Times Company**, and The McClatchy Company owns 10 percent or more of its stock.

**Tribune Publishing Company** is publicly held. Oaktree Tribune, L.P., owns 10 percent or more of Tribune Publishing Company's stock.

**Verband Deutscher Zeitschriftenverleger (VDZ)**, the umbrella organization for the German Magazine Publishers Association, has no parent company, and no publicly owned company owns any stock in the organization.

Nash Holdings LLC is the sole parent of WP Company LLC (d/b/a **The Washington Post**). Nash Holdings LLC is privately held and does not have any outstanding securities in the hands of the public.

## TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENTS.....	i
TABLE OF AUTHORITIES.....	vii
INTEREST OF <i>AMICI</i> .....	1
SUMMARY OF ARGUMENT.....	2
ARGUMENT.....	7
I.    A Subscriber’s Emails Are Not the “Business Records” of Its Email Service Provider .....	7
II.   The Distinction Between “Warrants” and “Subpoenas” Is Meaningful .....	17
III.  The District Court’s Opinion Sets a Dangerous International Precedent .....	28
CONCLUSION.....	34
CERTIFICATE OF COMPLIANCE .....	35
ADDENDUM: DESCRIPTIONS OF <i>AMICI CURIAE</i> .....	36

**TABLE OF AUTHORITIES**

<b>Cases</b>	<b>Page(s)</b>
<i>Amazon.com LLC v. Lay</i> , 758 F. Supp. 2d 1154 (W.D. Wash. 2010) .....	16
<i>Associated Press v. United States</i> , 326 U.S. 1 (1945).....	10
<i>Branzburg v. Hayes</i> , 408 U.S. 665 (1972).....	3, 9
<i>FAA v. Cooper</i> , 132 S. Ct. 1441 (2012).....	18
<i>Food Lion, Inc. v. Capital Cities/ABC</i> , No. 6:92CV00592, 1996 WL 575946 (M.D.N.C. Sept. 6, 1995) .....	15
<i>Gonzales v. National Broad. Co.</i> , 194 F.3d 29 (2d Cir. 1998) .....	27
<i>In the Matter of a Warrant to Search a Certain E-Mail Account controlled and Maintained by Microsoft Corporation</i> , 15 F. Supp. 3d 466 (S.D.N.Y. Apr. 25, 2014) .....	5
<i>In re Applications for Search Warrants for Info. Associated with Target Email Address</i> , No. 12-MJ-8119-DJW, 2012 WL 4383917 (D. Kan. Sept. 21, 2012).....	26
<i>In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461</i> , 706 F. Supp. 2d 11 (D.D.C. 2009).....	16
<i>In re Grand Jury Subpoena (Amazon.com)</i> , 246 F.R.D. 570 (W.D. Wis. 2007).....	16
<i>In re Grand Jury Subpoena to Kramerbooks &amp; Afterwords, Inc.</i> , 26 Media L. Rep. 1599 (D.D.C. 1988).....	16
<i>Klayman v. Obama</i> , 957 F. Supp. 2d 1 (D.D.C. 2013).....	12

*Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of New York Harbor*,  
667 F.2d 267 (2d Cir. 1981) .....15

*New York Times v. Gonzales*,  
459 F.3d 160 (2d Cir. 2006) .....12, 13, 14

*Philip Morris Cos. v. ABC, Inc.*,  
No. LX-816-3, 1995 WL 1055921 (Va. Cir. Ct. July 11, 1995) .....16

*Philip Morris Cos. v. ABC, Inc.*,  
No. LX-816-3, 1995 WL 301428 (Va. Cir. Ct. Jan. 26, 1995) .....15, 16

*Riley v. California*,  
134 S. Ct. 2473 (2014).....7, 8

*Stanford v. Texas*,  
379 U.S. 476 (1965).....26

*United States v. Burke*,  
700 F.2d 70 (2d Cir. 1983) .....27

*United States v. Odeh (In re Terrorist Bombings of U.S. Embassies)*,  
552 F.3d 157 (2d Cir. 2008) .....18

*United States v. Warshak*,  
631 F.3d 266 (6th Cir. 2010).....8

*Zurcher v. Stanford Daily*,  
436 U.S. 547 (1978).....19, 20, 26

**Federal Statutes**

18 U.S.C. § 2703.....*passim*

42 U.S.C. § 2000aa.....*passim*

**Regulations**

28 C.F.R. § 50.10 .....5, 23, 24

## Other Authorities

- Adrienne LaFrance, *The Tor Project helps journalists and whistleblowers go online without leaving a trace*, Nieman Lab (June 19, 2012), available at <http://bit.ly/1A5Dsia>.....14
- Ann E. Marimow, *A Rare Peek into a Justice Department Leak Probe*, Washington Post (May 19, 2013), available at <http://wapo.st/N1Qzh6>.....22
- Associated Press, *U.S.: C.I.A. Thwarts New Al-Qaeda Underwear Bomb Plot* (May 7, 2012), available at <http://usat.ly/1rDsalG> .....11
- Bruce Brown, *Press Subpoenas are a bigger problem than you'd think*, Columbia Journalism Rev. (Nov. 24, 2014), available at <http://bit.ly/1y9glUo>.....3
- Chris Brummit, *Vietnam's 'cyber troops' take fight to U.S., France*, Associated Press (Jan. 20, 2014), available at <http://bit.ly/1uVl4>.....30
- Cory Bennett, *Obama urges China to stop cyber theft*, The Hill (Nov. 10, 2014), available at <http://bit.ly/1w8KAM1>.....31
- Craig Timberg and Ellen Nakashima, *Chinese Hackers Suspected in Attack on The Post's Computers*, Washington Post (Feb. 1, 2013), available at <http://wapo.st/1yr2Oqw> .....29
- Craig Timberg, *Foreign regimes use spyware against journalists, even in U.S.*, Washington Post (Feb. 12, 2014), available at <http://wapo.st/McG3TZ>.....30
- Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Washington Post (Nov. 2, 2005), available at <http://wapo.st/1fk1wVN>.....10
- David Von Drehle, *FBI's No. 2 Was 'Deep Throat': Mark Felt Ends 30-Year Mystery of the Post's Watergate Source*, Washington Post (June 1, 2005), available at <http://wapo.st/1ok8ZXe> .....10

Denise Lu, <i>Freedom of the Press Foundation Steps Up Encryption Efforts for Journalists</i> , PBS MediaShift (Dec. 16, 2013), available at <a href="http://to.pbs.org/18NBYua">http://to.pbs.org/18NBYua</a> .....	14
Dep't of Justice, <i>U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage</i> , May 19, 2014, available at <a href="http://1.usa.gov/1py">http://1.usa.gov/1py</a> .....	31
Dylan Byers, <i>Reporters Say There's a Chill in the Air</i> , Politico (June 8, 2013), available at <a href="http://politi.co/1AFcj8N">http://politi.co/1AFcj8N</a> .....	32
FRONTLINE (PBS), <i>News War</i> , Feb. 13, 2007, available at <a href="http://to.pbs.org/124RCVI">http://to.pbs.org/124RCVI</a> .....	11
James Risen and Eric Lichtblau, <i>Bush Lets U.S. Spy on Callers Without Courts</i> , N.Y. Times (Dec. 16, 2005), available at <a href="http://nyti.ms/1y8izFc">http://nyti.ms/1y8izFc</a> ; .....	10
Jane Mayer, <i>What's the Matter with Metadata?</i> , The New Yorker (June 6, 2013), available at <a href="http://nyr.kr/1cXSD2V">http://nyr.kr/1cXSD2V</a> .....	12
Jeremy Barr, <i>How Journalists Can Encrypt Their Email</i> , Poynter (Dec. 19, 2013), available at <a href="http://bit.ly/1ya6v6c">http://bit.ly/1ya6v6c</a> .....	14
Jeremy Wagstaff, <i>Journalists, media under attack from hackers: Google researchers</i> , Reuters (Mar. 28, 2014), available at <a href="http://reut.rs/1I9SpbW">http://reut.rs/1I9SpbW</a> .....	30
Lauren Kirchner, <i>Encryption, Security Basics for Journalists</i> , Columbia Journalism Review (Sept. 17, 2013), available at <a href="http://bit.ly/1y6e6l6">http://bit.ly/1y6e6l6</a> .....	14
Leonard Downie Jr. and Sara Rafsky, <i>The Obama Administration and the Press</i> , Committee to Protect Journalists (Oct. 10, 2013), available at <a href="http://bit.ly/1dZ4w5P">http://bit.ly/1dZ4w5P</a> .....	32
Mark Sherman, <i>Gov't Obtains Wide AP Phone Records in Probe</i> , Associated Press (May 13, 2013), available at <a href="http://bit.ly/1Iz5sNG">http://bit.ly/1Iz5sNG</a> .....	23

Michael Isikoff, *DOJ confirms Holder OK'd search warrant for Fox News reporter's emails*, NBC News (May 23, 2013), available at <http://nbcnews.to/1tEoJW1> .....22

Michael Tarm, *Journalists criticize White House for 'secrecy,'* Associated Press (Sept. 17, 2014), available at <http://bit.ly/1uWA7Pw> .....32

Nick Hopkins and Luke Harding, *Pro-Assad Syrian hackers launching cyber-attacks on Western media*, The Guardian (Apr. 29, 2013), available at <http://bit.ly/1xVALNa>.....30

Nicole Perloth, *Hackers in China Attacked the Times for Last Four Months*, N.Y. Times (Jan. 30, 2013), available at <http://nyti.ms/1pVnfev> .....29

Scott Shane, David Johnston, and James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007), available at <http://nyti.ms/1vX7XJ0> .....10

Siobhan Gorman, Devlin Barrett and Danny Yadron, *Chinese Hackers Hit U.S. Media*, Wall Street Journal (Jan. 31, 2013), available at <http://on.wsj.com/1rIBDbj>.....29

Stephen Bates, *The Reporter's Privilege, Then and Now*, Joan Shorenstein Center for Press, Politics and Public Policy, Harvard University John F. Kennedy School of Government (April 2007) .....3, 23

Suman Varandani, *U.S. Refuses to 'Stand Idle' in Charging China Over Government-Backed Cyberattacks*, International Business Times (Nov. 11, 2014), available at <http://bit.ly/1vF7GqS> .....31

Associated Press, *'Syrian Electronic Army' takes credit for hacking New York Times website* (Aug. 27, 2013), available at <http://cbsn.ws/1rF615f> .....30



*With Liberty to Monitor All: How Large-Scale U.S. Surveillance Is  
Harming Journalism, Law, and American Democracy*, Human  
Rights Watch/ACLU (July 2014),  
available at <http://bit.ly/1zp> .....33

### INTEREST OF AMICI<sup>1</sup>

*Amici* are 29 leading U.S. and foreign news organizations and trade organizations that support and represent journalists and publishers worldwide (collectively, “Media Amici”).<sup>2</sup> In their daily work of reporting and publishing from every corner of the globe, Media Amici rely on the email and cloud-storage services provided by Microsoft, Google, Amazon and others to carry on confidential communications with sources; to gather, store and review documents; and to draft articles reporting on the major issues of our day. They also rely on the protections of U.S. law that have restricted the government’s ability to search the newsroom for information, whether that newsroom is in a physical building or hosted remotely in the cloud.

---

<sup>1</sup> Pursuant to Fed. R. App. P. 29(c)(5) and Local Rule 29.1, undersigned counsel for Media Amici hereby certify that no party’s counsel authored the brief in whole or in part. No party or party’s counsel contributed money that was intended to fund preparing or submitting the brief. No person, other than the Media Amici, their members, or their counsel, contributed money that was intended to fund preparing or submitting the brief. All parties have consented to the filing of this brief.

<sup>2</sup> The Addendum to this brief contains a complete description of each *amicus* party.

Media Amici are concerned that the district court's decision, if upheld, will undermine procedural and substantive protections for material that is protected by the First Amendment. Even if the subscriber today is not a reporter—although we do not know for sure—the next subscriber may be. For the reasons explained below, Media Amici urge this Court to reverse the district court's decision.

### **SUMMARY OF ARGUMENT**

Modern journalism is a global, networked endeavor. Journalists gather the news and file their stories from all corners of the globe—and may rarely set foot in a brick-and-mortar newsroom. They communicate with sources by email on mobile devices and laptop computers; they store and share newsgathering materials in cloud-based storage services; and they draft, edit and submit articles remotely. But though the technology is new, the threats are as old as our nation: whether it is a colonial governor seeking the identity of John Peter Zenger's anonymous columnists or the Nixon administration seeking reporters' notes of interactions with the

Weathermen and the Black Panthers,<sup>3</sup> governments still seek to “annex the journalistic profession as an investigative arm of government,” demanding the materials they have gathered and drafted in the course of reporting the news. *Branzburg v. Hayes*, 408 U.S. 665, 725 (1972) (Stewart, J., dissenting).<sup>4</sup>

As Microsoft lays out in the opening pages of its brief, one need only imagine that the records sought by the government are a reporter’s communications to appreciate the obvious dangers inherent in the district court’s decision. Taken to its logical conclusion, the district court’s decision would allow the U.S. government to obtain a warrant *ex parte* and seize from a service provider a reporter’s newsgathering materials anywhere in the world—and would defeat attempts to dissuade other countries from seeking the emails of a U.S. reporter stored on U.S. soil by accessing the reporter’s account from overseas.

This is a dangerous precedent to set. Extant law protects newsgathering materials from search and seizure by the government,

---

<sup>3</sup> See Stephen Bates, *The Reporter’s Privilege, Then and Now*, Joan Shorenstein Center for Press, Politics and Public Policy, Harvard University John F. Kennedy School of Government (April 2007), at 4.

<sup>4</sup> See also Bruce Brown, *Press Subpoenas are a bigger problem than you’d think*, *Columbia Journalism Rev.* (Nov. 24, 2014), available at <http://bit.ly/1y9glUo>.

except under very narrow circumstances. Even if this warrant's target is not a reporter, the next target easily could be. Media Amici therefore urge this Court to consider the impact of this decision on the First Amendment protections for records of journalists that are necessarily held by third-party service providers.

The district court's decision is deeply troubling to Media Amici for three reasons.

*First*, the district court's decision relies on the erroneous—and dangerous—assumption that the contents of an individual's email, stored and transmitted by a service provider like Microsoft, are the “business records” of Microsoft—not the personal, private records of the individual customer. This is a particular concern for Media Amici, since those documents that the district court would consider Microsoft's “business records” would necessarily include newsgathering materials and communications with sources, protected by the First Amendment. A modern news organization has its newsroom in the cloud and expects that the electronic walls to that newsroom are as secure from third-party intrusion as physical walls have been. Media Amici are concerned that by characterizing the contents of communications as Microsoft's “business

records” susceptible to production through a subpoena-warrant “hybrid,” the District Court’s holding throws into question the scope and extent of the First Amendment protections to which these communications are entitled.

*Second*, by endorsing the government’s position that a warrant pursuant to 18 U.S.C. § 2703(a) is no “warrant” at all, but rather a “hybrid” that is “part search warrant and part subpoena,”<sup>5</sup> the district court erodes the legal distinctions between these two forms of process and leaves us with the worst of both worlds—expansive scope and uncertain rules. But the distinction between warrants and subpoenas is a meaningful one, and it appears in key regulations and laws affecting the government’s ability to obtain information from members of the media. In particular, the court’s formulation of a “hybrid” subpoena-warrant combination—issued like a warrant, executed like a subpoena—muddies the protections of the Privacy Protection Act, 42 U.S.C. § 2000aa, and the recently revised DOJ policies, codified at 28 C.F.R. § 50.10 (the “DOJ Media Policy”), which rely on these

---

<sup>5</sup> *In the Matter of a Warrant to Search a Certain E-Mail Account controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 471 (S.D.N.Y. Apr. 25, 2014).

terms and secure a presumption of notice and an opportunity to challenge. At the very least, any decision should be limited to avoid needlessly complicating these long-defined terms and inviting conflict with these restrictions on government access.

*Finally*, Media Amici stress to this Court that the danger of foreign governments seeking documents held beyond their own borders is real. Media organizations and writers are frequently the target of hacking, surveillance, and raids by authoritarian governments that would love nothing more than to access the emails of U.S. journalists who report within their borders but store their emails in the United States and more protective nations. By allowing the U.S. government to compel Microsoft to search and produce a subscriber's emails stored in foreign venues, the district court's opinion opens the door for foreign authorities to demand that Microsoft's local subsidiary produce the records of U.S.-based journalists.

## ARGUMENT

### I. A Subscriber's Emails Are Not the "Business Records" of Its Email Service Provider

Media Amici are deeply troubled by the district court's holding that emails and other electronic files stored remotely with Microsoft and other service providers are the "business records" of those service providers and are therefore appropriately obtained through an *ex parte* subpoena-like process.<sup>6</sup> This assumption is wrong and dangerous.

Federal courts have recognized that our private electronic documents are our own, even when technically accessible by the third-party service provider that stores and maintains them on our behalf by contractual arrangement. Writing for a unanimous Supreme Court in *Riley v. California*, 134 S. Ct. 2473 (2014), Chief Justice Roberts explained that an individual's emails and electronic files contain a "cache of sensitive personal information" — "[t]he sum of an individual's private life,"

---

<sup>6</sup> At oral argument, the district court declined to consider Microsoft's argument that such records "are not Microsoft's documents but the documents of its customers," believing that the argument was waived for not having been raised below. That argument had, in fact, been raised below and figured prominently in Microsoft's briefing before the magistrate judge. See Brief of Appellant Microsoft Corp. ("Microsoft Br.") at 53 n.7.



including “a record of all his communications” and “a thousand photographs.” *Id.* at 2489-90. Electronic devices serve as “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” *Riley*, 134 S. Ct. at 2489. Indeed, messages stored in an individual’s email account “provide[] an account of its owner’s life,” such that “[b]y obtaining access to someone’s email, government agents gain the ability to peer deeply into his activities.” *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

Increasingly, this private information is maintained by service providers in the cloud, “stored on remote servers rather than on the device itself.” *Riley*, 134 S. Ct. at 2491. In this way, internet service providers have become the “functional equivalent of a post office or a telephone company,” passing along private messages to which they are not a party. *Warshak*, 631 F.3d at 286.

By assuming that the emails targeted by this warrant are Microsoft’s business records—rather than the records of the individual account-holder—the district court’s opinion raises serious Fourth Amendment

concerns for anyone who uses email or maintains documents in the cloud.<sup>7</sup> As *Warshak* illustrates, the contents of communications are entitled to Fourth Amendment protections. These protections are also part of the important procedural and substantive protections afforded to materials protected by the First Amendment. When the account-holder in question is a member of the press, these concerns are magnified even further. The district court's logic would extend not only to reporters' emails, but to interview notes, outlines, contact lists, and article drafts stored by a service provider. Such documents would provide a road map to a reporter's confidential sources and investigative process.

Protecting confidential sources and the newsgathering process has always been a paramount concern for the press. A necessary corollary of the First Amendment right to publish the news is a right to gather it; as the Supreme Court recognized, "without some protection for seeking out the news, freedom of the press could be eviscerated." *Branzburg*, 408 U.S. at

---

<sup>7</sup> These privacy concerns were raised by *amici* below, including the Electronic Frontier Foundation. Because Media Amici expect that other *amici* will address in depth the Fourth Amendment issues raised by this case, Media Amici will not repeat those arguments here. Instead, Media Amici focus in this brief on the serious *First* Amendment concerns that are also raised by the district court's holding.

680. And just as “[a] free press is indispensable to the workings of our democratic society,” “confidential sources are essential to the workings of the press.” *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1183 (D.C. Cir. 2006) (Tatel, J., concurring) (quoting *Associated Press v. United States*, 326 U.S. 1, 28 (1945) (Frankfurter, J., concurring)).

Confidential sources are a hallmark of reporting on major stories of public importance. For example:

- Washington Post reporters Bob Woodward and Carl Bernstein reported the break-ins at the Watergate Hotel by relying on “Deep Throat,” a confidential source whose identity the reporters guarded for over thirty years. David Von Drehle, *FBI’s No. 2 Was ‘Deep Throat’: Mark Felt Ends 30-Year Mystery of the Post’s Watergate Source*, Washington Post (June 1, 2005), available at <http://wapo.st/1ok8ZXe>.
- The New York Times used confidential sources to break the story that then-President George W. Bush secretly authorized the National Security Agency to monitor phone calls and email messages of individuals in the United States without obtaining warrants, and to report on the Bush Administration’s approval of harsh interrogation tactics for terrorism suspects. James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), available at <http://nyti.ms/1y8izFc>; Scott Shane, David Johnston, and James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007), available at <http://nyti.ms/1vX7XJ0>.
- The Washington Post relied on confidential sources to break the news that the CIA detained and interrogated terrorism suspects at secret “black sites” in Eastern Europe. Dana Priest, *CIA*

*Holds Terror Suspects in Secret Prisons*, Washington Post (Nov. 2, 2005), available at <http://wapo.st/1fk1wVN>.

- The Associated Press relied on confidential government sources to reveal a foiled terror plot in Yemen. Associated Press, *U.S.: C.I.A. Thwarts New Al-Qaeda Underwear Bomb Plot* (May 7, 2012), available at <http://usat.ly/1rDsalG>.

And the list goes on. Indeed, as Carl Bernstein noted in a FRONTLINE interview several years ago: “I know of very little reporting of the last 30 to 40 years that has been done without use of confidential sources, particularly in the national security area.” FRONTLINE (PBS), *News War*, Feb. 13, 2007, available at <http://to.pbs.org/124RCVI>.

But a promise of confidentiality is worth little if a reporter’s emails and electronic documents can be plucked from the cloud by simply compelling a third-party service provider to turn them over, without ever examining the First Amendment issues raised by such a compelled production. In the course of gathering the news, reporters must interact with the modern world—they must travel, eat, contact sources, consult maps, and purchase books. Each of these actions necessarily creates an

electronic bread crumb which, taken together, can provide a road map to a reporter's movements, research and interactions.<sup>8</sup>

If the emails sought by the government in this case are those of a reporter, simply calling them Microsoft's "business records" – which they are not—still would not permit the government to perform an end run around the important First Amendment and common-law protections for newsgathering materials.

Recognizing that the tools of modern newsgathering necessarily deposit records with third parties, this Court made clear in *New York Times v. Gonzales*, 459 F.3d 160 (2d Cir. 2006), that protections for a reporter's confidential information extend to third-party holders of that information. After unsuccessfully seeking the phone records of two New York Times reporters directly from the newspaper in a leak investigation, the government threatened to obtain the phone records directly from the

---

<sup>8</sup> As Jane Mayer noted in *The New Yorker*, today's metadata can be "revelatory" – potentially more so than the content of a communication itself. Jane Mayer, *What's the Matter with Metadata?*, *The New Yorker* (June 6, 2013), available at <http://nyr.kr/1cXSD2V>. See also *Klayman v. Obama*, 957 F. Supp. 2d 1, 36 (D.D.C. 2013) (noting that "[r]ecords that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life"), appeal pending, Nos. 14-5004, 14-5005, 14-5016, 14-5017 (D.C. Cir. argued Nov. 4, 2014).

newspaper's telephone provider. The Times brought a declaratory action, asking the court to recognize that the same privileges that protected its reporters from disclosing their own records extended to records in the possession of the third-party phone company. The Second Circuit agreed, holding that "so long as the third party plays an 'integral role' in reporters' work, the records of third parties detailing that work are, when sought by the government, covered by the same privileges afforded to the reporters themselves and their personal records." *Gonzales*, 459 F.3d at 168.

Judge Sack agreed with the legal conclusion that reporters' confidential materials are protected even when held by third parties, though he dissented from the majority's ultimate finding that the privilege had been overcome on the facts of the case (*id.* at 174). Without such protection for newsgathering materials held by service providers, Judge Sack warned:

Reporters might find themselves, as a matter of practical necessity, contacting sources the way ... drug dealers reach theirs—by use of clandestine cell phones and meetings in darkened doorways. Ordinary use of the telephone could become a threat to journalist and source alike. It is difficult to see in whose best interests such a regime would operate.

*Id.* at 175 (Sack, J., dissenting). This is the world that would result from holding that a reporter's emails should be considered the "business records" of his or her email service provider, subject to compelled disclosure worldwide without notice to the reporter.<sup>9</sup> It is disturbingly unclear whether the warrant-subpoena "hybrid" process proposed by the district court could take into account the important First Amendment concerns that *Gonzales* addresses.

Other courts have similarly recognized that records held by third parties can implicate First Amendment concerns. Prior to *Gonzales*, the Second Circuit held that a subpoena to a third-party payroll provider seeking the names of union members who had recently authorized contributions to the union's political action committee implicated the union

---

<sup>9</sup> Indeed, the world described by Judge Sack is already becoming a reality, as journalists are increasingly turning to encryption and to anonymizing software such as Tor in order to protect their newsgathering and source contacts from government surveillance. See, e.g., Lauren Kirchner, *Encryption, Security Basics for Journalists*, Columbia Journalism Review (Sept. 17, 2013), available at <http://bit.ly/1y6e6l6>; Jeremy Barr, *How Journalists Can Encrypt Their Email*, Poynter (Dec. 19, 2013), available at <http://bit.ly/1ya6v6c>; Denise Lu, *Freedom of the Press Foundation Steps Up Encryption Efforts for Journalists*, PBS MediaShift (Dec. 16, 2013), available at <http://to.pbs.org/18NBYua>; Adrienne LaFrance, *The Tor Project helps journalists and whistleblowers go online without leaving a trace*, Nieman Lab (June 19, 2012), available at <http://bit.ly/1A5Dsia>.

members' First Amendment rights. *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of New York Harbor*, 667 F.2d 267, 271 (2d Cir. 1981). In *Food Lion, Inc. v. Capital Cities/ABC*, the Food Lion supermarket chain sought records from hotels, letter-carrier services, and telecommunications companies, in an attempt to reconstruct the investigative processes of undercover reporters from ABC News who reported on the store's unsanitary practices. No. 6:92CV00592, 1996 WL 575946, at \*1 (M.D.N.C. Sept. 6, 1995), *aff'd*, 951 F. Supp. 1211 (M.D.N.C. 1996). Even though the subpoena requests were targeted to third parties—not ABC directly—the court found that the discovery “improperly infringe[d]” on ABC's First Amendment rights since it could potentially reveal the reporters' confidential sources. *Id.* at \*2.

Similarly, in *Philip Morris Cos. v. ABC, Inc.*, tobacco company Philip Morris tried to unmask a confidential source interviewed by ABC using a series of third-party subpoenas on phone, credit card, hotel and airline companies, seeking receipts and records that might help trace the source. ABC moved to quash the subpoenas, arguing that this effort to ferret out a source's identity is “tantamount to asking the reporter himself to divulge the identity of his confidential sources,” and that this practice would chill



the “constitutionally protected functions” of newsgathering since “reporters must travel and use the telephone in order to gather the news, and foster the free flow of information.” No. LX-816-3, 1995 WL 301428, at \*6 (Va. Cir. Ct. Jan. 26, 1995). The court ultimately denied the requested discovery, finding that Philip Morris had not overcome ABC’s qualified privilege in the newsgathering materials. *Philip Morris Cos. v. ABC, Inc.*, No. LX-816-3, 1995 WL 1055921 (Va. Cir. Ct. July 11, 1995).<sup>10</sup>

Although these cases involved civil subpoenas rather than government warrants, they nevertheless stand for the proposition that First Amendment concerns are implicated where legal process is used to get

---

<sup>10</sup> Similarly, courts have repeatedly rejected attempts by the government to compel third parties to disclose what an individual reads or listens to, citing First Amendment concerns. *See, e.g., In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. 1599, 1600 (D.D.C. 1988) (subpoena seeking Monica Lewinsky’s book purchases implicated First Amendment); *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461*, 706 F. Supp. 2d 11 (D.D.C. 2009) (refusing to compel disclosure of adult-video company’s customers where government failed to demonstrate compelling need for First Amendment-protected information); *In re Grand Jury Subpoena (Amazon.com)*, 246 F.R.D. 570, 572-73 (W.D. Wis. 2007) (refusing to compel Amazon to disclose the names of customers who had purchased particular books, CDs and DVDs from the retailer); *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1167 (W.D. Wash. 2010) (rejecting North Carolina revenue department’s demand that Amazon disclose customers’ book purchases).

records held by third parties. In short, it is plain that reporters, like other individuals, retain a First Amendment right in their own information even where it is held by third-party providers—and seeking that information directly from a third-party service provider on the assumption that it is the *service provider's* information to disclose raises serious First Amendment issues. The concerns are even more dramatic for those Media Amici with foreign-based operations and reporters, whose reporters' information is likely stored on servers outside the United States. The district court's decision transforms these materials from the newsgathering documents of a foreign news organization to the "business records" of a U.S.-based service provider.

In sum, the emails sought here are not the "business records" of Microsoft; but even if they were, the government should not be able to perform an end run around First Amendment protections for the press simply by characterizing them as such.

## **II. The Distinction Between "Warrants" and "Subpoenas" Is Meaningful**

"[I]t is a cardinal rule of statutory construction that, when Congress employs a term of art, it presumably knows and adopts the cluster of ideas

that were attached” to that term. *FAA v. Cooper*, 132 S. Ct. 1441, 1449 (2012) (internal quotation marks and citations omitted). The term “warrant” carries it with a defined “cluster of ideas”—which include the understanding that it cannot be enforced extraterritorially. *See United States v. Odeh (In re Terrorist Bombings of U.S. Embassies)*, 552 F.3d 157, 169 (2d Cir. 2008). *See also* Microsoft Br. at 21-22.

There is a whole regime of statutes and regulations guarding the media against unwarranted intrusion into newsgathering activities—and this regime repeatedly refers to protections in place when documents are sought by warrant or by subpoena. By suggesting that a Section 2703(a) warrant is really a subpoena—or a subpoena-warrant “hybrid”—the district court’s order makes these long-defined terms unclear and introduces needless uncertainty about the protections that this regime affords.

For example, the Privacy Protection Act (“PPA”), 42 U.S.C. § 2000aa, makes it unlawful for a government officer “*to search for or seize* any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.” 42 U.S.C. § 2000aa(a)

(emphasis added). The PPA generally prohibits the government from searching for certain newsgathering materials—including anything would reflect the “mental impressions, conclusions, opinions, or theories”<sup>11</sup>—in a criminal case.

Congress passed the PPA in response to the Supreme Court’s decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). See S. Rep. No. 96-874, at 4 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3950 (1980). *Zurcher* arose when police obtained a warrant to search the *Stanford Daily*’s newsroom, seeking unpublished photos for evidence of a crime. The officers searched the newspaper’s “photographic laboratories, filing cabinets, desks, and wastepaper baskets,” and reviewed notes and correspondence—but ultimately found no unpublished photographs to seize. *Zurcher*, 436 U.S. at 551. The newspaper brought suit against the police department for First and Fourth Amendment violations, and won declaratory relief from the district court and the Ninth Circuit. But the Supreme Court reversed. It declined to read the Fourth Amendment “to impose a general constitutional barrier against warrants to search

---

<sup>11</sup> 42 U.S.C. § 2000aa-7(b).

newspaper premises, to require resort to subpoenas as a general rule, or to demand prior notice and hearing in connection with the issuance of search warrants. *Id.* at 567.

The Supreme Court's refusal to bar newsroom search warrants on constitutional grounds generated a public outcry and spurred legislative action. S. Rep. No. 96-874 at 5-6, 1980 U.S.C.C.A.N. at 3951-52. The resulting law bans search warrants where the materials sought are "work product" materials, and enacts a "subpoena-first" rule where the government seeks "documentary materials."<sup>12</sup> 42 U.S.C. § 2000aa; *see also* S. Rep. No. 96-874, at 9, 1980 U.S.C.C.A.N. at 3956 ("When the materials sought consist of work product, a general no-search rule applies. When the materials sought constitute documentary materials other than work product, a subpoena-first rule is generally applicable.") In narrow

---

<sup>12</sup> The statute defines "work product" materials to include materials that are "prepared, produced, authored, or created" in anticipation of dissemination to the public and which reflect the preparing party's "mental impressions, conclusions, opinions, or theories." 42 U.S.C. § 2000aa-7(b). "Documentary materials" include "materials upon which information is recorded"—such as photographs, video, audio recordings, and printed materials—that are gathered in anticipation of publication, but which are not created in anticipation of publication and do not reflect the author's mental impressions. 42 U.S.C. § 2000aa-7(a).

circumstances where certain materials cannot be obtained by subpoena and delay would “threaten the interests of justice,” the government may proceed by warrant *provided that* it allows the news organization notice and an opportunity to contest the seizure in court. 42 U.S.C. § 2000aa(b)(4)(c). In short, the mechanics of the PPA clearly differentiate between a “warrant” and a “subpoena” —*prohibiting* search and seizure of work product and newsgathering materials by warrant, except in rare instances and then with notice to the news organization, and *requiring* a “subpoena-first” approach for documentary materials.<sup>13</sup> The district court’s holding could dilute the protections of the PPA by calling into question whether a Section 2703(a) warrant—like any other warrant—is subject to the PPA’s restrictions, or whether it is really a subpoena.

Prior to this decision, the government has demonstrated that it considers Section 2703(a) warrants to trigger the PPA’s restrictions. When the government sought a warrant to compel Google to turn over the content of emails belonging to Fox News journalist James Rosen—seeking

---

<sup>13</sup> The PPA contains a narrow “suspect” exception: a warranted search is permitted where there is probable cause to believe the person possessing the newsgathering materials committed the crime that the government is investigating and to which the materials relate.

to identify a confidential government source who had allegedly provided classified information about North Korea<sup>14</sup>—it submitted an affidavit invoking *both* section 2703(a) of ECPA and the PPA. See Affidavit of Reginald B. Reyes in Support of Application for Search Warrant, ECF No. 20-1, *Application for Search Warrant for E-Mail Account [REDACTED]@gmail.com Maintained on Computer Servers Operated by Google, Inc.*, No. 10 Mag. 291 (D.D.C. Nov. 7, 2011), ¶ 3. The government alleged that Rosen violated the Espionage Act as an “aider and abettor and/or co-conspirator” in order to fit within the PPA’s narrow “suspect” exception to its general prohibition against warranted searches and seizures of newsrooms.<sup>15</sup> *Id.* ¶¶ 5, 8.

News of the Rosen warrant—coming in the same month that the Associated Press learned that the government had secretly obtained

---

<sup>14</sup> See Ann E. Marimow, *A Rare Peek into a Justice Department Leak Probe*, Washington Post (May 19, 2013), available at <http://wapo.st/N1Qzh6>.

<sup>15</sup> See also Michael Isikoff, *DOJ confirms Holder OK'd search warrant for Fox News reporter's emails*, NBC News (May 23, 2013), available at <http://nbcnews.to/1tEoJW1> (reporting government's statement that Rosen warrant was intended to comply with the Privacy Protection Act).

telephone records for its reporters<sup>16</sup>—caused a public and media outcry. In response, the Justice Department revised its internal policies—first enacted in response to an earlier “subpoena epidemic” during the Nixon administration<sup>17</sup>—for seeking information from members of the news media.

The recently revised DOJ policies on seeking information from the media further underscore the distinction between warrants and subpoenas. Like the PPA, the newly revised DOJ Media Policy turns on distinctions between “subpoenas”—which are grouped with civil investigative demands, pen register orders under 18 U.S.C. § 3123, and Section 2703(d) orders (*see* 28 C.F.R. § 50.10(b)(2)(i))—and “warrants,” which include Rule 41 warrants as well as warrants “to obtain from third-party ‘communications service providers’ the communications records of members of the news media, pursuant to 18 U.S.C. 2703(a) and (b).” 28 C.F.R. § 50.10(b)(2)(ii). The strong presumption of notice to the news media and an opportunity to challenge can only be overcome if the

---

<sup>16</sup> *See* Mark Sherman, *Gov’t Obtains Wide AP Phone Records in Probe*, Associated Press (May 13, 2013), *available at* <http://bit.ly/11Z5sNG>.

<sup>17</sup> Bates, *supra* note 3, at 4.



Attorney General determines that, “for *compelling* reasons,” notice would “pose a *clear and substantial threat* to the integrity of the investigation” (which does not include merely delaying the investigation), “risk *grave harm* to national security, or present an *imminent* risk of death or of serious bodily harm.” 28 C.F.R. § 50.10(e)(1) (emphasis added).

The DOJ Media Policy makes clear that Section 2703(a) warrants fall within the scope of the PPA’s restrictions.<sup>18</sup> In subsection (d), the Media Policy narrows the scope of the PPA’s “suspect exception,” clarifying that government may not “apply for a warrant” for PPA-protected materials where the journalist is a “suspect” based on his newsgathering activities, or to further the investigation of a “suspect” *other* than the journalist. 28 C.F.R. § 50.10(d)(4) & (5).

The district court’s interpretation of Section 2703(a) warrants—that such warrants are not “warrants” at all, but a hybrid form of process without the protections of notice or opportunity to be heard—threatens to undercut the heightened requirements for warranted searches of electronic

---

<sup>18</sup> In the rare instances that a warrant is permitted, the PPA specifically requires notice to the news organization to challenge—protections which the warrant issued to Microsoft specifically prohibits. See Microsoft Br. at 29 (warrant allows 30-day delay in notification to subscriber).

newsgathering documents imposed by the PPA and the DOJ Media Policy. Allowing courts to pick and choose among the attributes of a “warrant” starts a long slide down a slippery slope toward the types of broadly worded “general warrants” that the Fourth Amendment was enacted to prohibit. While the PPA and the DOJ Media Policy are important defenses, they are subject to limitations. Neither tool provides news organizations with an affirmative right to intervene and challenge unlawful, overbroad searches prior to execution. It is therefore crucial to Media Amici that courts do not relax the clearly defined requirements for seeking and executing a warrant, and do not create a new “hybrid” form of process that would potentially throw existing protections into question.

Moreover, it is far from clear that the district court in this case considered the important First Amendment issues raised by the broad scope of this warrant—which calls for the production of “all emails.” This is exactly the kind of fishing expedition that runs counter to the protections of *both* the First and Fourth Amendments. The warrant lacks any semblance of particularity when it calls for “the contents of all e-mails” stored in the user’s account (including sent emails), as well as “[a]ll records or other information stored by an individual using the account, including

address books, contact and buddy lists, pictures, and files," from the time the account was opened until the present. *See* Appendix at A46-48. The warrant states that the government will cull through this mountain of data using unspecified keyword searches, as well as "email-by-email review." Such a broad sweep of information does not pass First or Fourth Amendment muster.

In *Stanford v. Texas*, the Supreme Court invalidated a similarly overbroad warrant authorizing the search of a private home for all books, records, and other materials relating to the Communist Party, finding the warrant's "indiscriminate sweep" to be the functional equivalent of a "general warrant" – one of the principal targets of the Fourth Amendment. 379 U.S. 476 (1965). Rather, "[w]here presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field." *Zurcher*, 436 U.S. at 564. *See also, e.g., In re Applications for Search Warrants for Info. Associated with Target Email Address*, No. 12-MJ-8119-DJW, 2012 WL 4383917, at \*9 (D. Kan. Sept. 21, 2012) (denying as unconstitutional warrant under the Stored Communications Act seeking "content of every email or fax sent to or from" certain accounts).

This is particularly so when newsgathering materials are sought. In these instances, there must be a compelling need for the material; the case must rise and fall on the material; and other sources must be exhausted. *See, e.g., United States v. Burke*, 700 F.2d 70, 76-77 (2d Cir. 1983) (“The law in this Circuit is clear that to protect the important interests of reporters and the public in preserving the confidentiality of journalists’ sources, disclosure may be ordered only upon a clear and specific showing that the information is: highly material and relevant, necessary or critical to the maintenance of the claim, and not obtainable from other available sources.”); *Gonzales v. National Broad. Co.*, 194 F.3d 29, 35 (2d Cir. 1998) (holding that qualified reporter’s privilege applies to non-confidential, as well as confidential, newsgathering information, and cautioning that allowing “unrestricted, court-enforced access” to journalist’s files “would risk the symbolic harm of making journalists appear to be an investigative arm of the judicial system, the government, or private parties”). The broad undifferentiating sweep of the warrant meets none of these criteria. And the warrant here raises additional concerns, because third parties are often ill-equipped to raise First Amendment arguments on behalf of their users.

### **III. The District Court's Opinion Sets a Dangerous International Precedent**

Media Amici have newsgathering and reporting operations around the globe. The district court's opinion, if affirmed, would have very real—and dire—impacts on their ability to gather and report the news.

*First*, the district court's holding would set a dangerous precedent for foreign governments who already try to access the communications of U.S. journalists reporting politically sensitive stories. At oral argument, Microsoft pointed out to the court that just that week, Chinese authorities raided four Microsoft locations. The authorities took servers from Microsoft's offices and "demanded a password to seek email information in the United States." *See* Appendix at A314. Microsoft refused because the Chinese government did not have jurisdiction over emails located outside China.

The district court's decision undercuts that reasoning. If a U.S. court can compel a service provider to search and seize emails located anywhere in the world—without notifying either the subscriber or the sovereign nation where the emails and subscriber are located—other governments will demand the same response from those service providers' subsidiaries

in their own countries. In addition to seeking records from cloud providers, government authorities may raid local news bureaus seeking access to the emails of reporters based in the United States.

These are not academic concerns. U.S.-based journalists are already the frequent targets of state-sponsored hackers who attempt to obtain newsgathering information or otherwise retaliate for certain coverage. Last year, the New York Times revealed that Chinese hackers targeted the email accounts of New York Times reporters for months after the newspaper published an investigative report about the secret fortune accumulated by outgoing Chinese leader Wen Jiabao.<sup>19</sup> The Washington Post and the Wall Street Journal reported cyber-attacks from Chinese hackers during the same time period.<sup>20</sup> Pro-Assad hackers from the Syrian Electronic Army have repeatedly targeted news sites, including Forbes, NPR, the Associated Press, the New York Times, Reuters, the Washington Post, Time, Al

---

<sup>19</sup> Nicole Perloth, *Hackers in China Attacked the Times for Last Four Months*, N.Y. Times (Jan. 30, 2013), available at <http://nyti.ms/1pVnfev>.

<sup>20</sup> See Siobhan Gorman, Devlin Barrett and Danny Yadron, *Chinese Hackers Hit U.S. Media*, Wall Street Journal (Jan. 31, 2013), available at <http://on.wsj.com/1rIBDbj>; Craig Timberg and Ellen Nakashima, *Chinese Hackers Suspected in Attack on The Post's Computers*, Washington Post (Feb. 1, 2013), available at <http://wapo.st/1yr2Oqw>.

Jazeera, and CNN.<sup>21</sup> U.S.-based Ethiopian journalists have been targeted by hackers likely affiliated with the Ethiopian government,<sup>22</sup> and hackers associated with the Vietnamese government targeted an Associated Press reporter based in Hanoi.<sup>23</sup> The problem is widespread: In March 2014, two Google security engineers revealed that “[t]wenty-one of the world’s top-25 news organizations have been the target of likely state-sponsored hacking attacks.”<sup>24</sup>

For those countries that are already taking extra-legal measures to try to penetrate and monitor journalists’ emails, the district court’s opinion offers a far easier approach: simply raid the local office of a service provider and demand that a local employee retrieve the desired information remotely from U.S.-based accounts. This scenario would cause

---

<sup>21</sup> See, e.g., Associated Press, *‘Syrian Electronic Army’ takes credit for hacking New York Times website* (Aug. 27, 2013), available at <http://cbsn.ws/1rF6l5f>; Nick Hopkins and Luke Harding, *Pro-Assad Syrian hackers launching cyber-attacks on Western media*, *The Guardian* (Apr. 29, 2013), available at <http://bit.ly/1xVALNa>.

<sup>22</sup> Craig Timberg, *Foreign regimes use spyware against journalists, even in U.S.*, *Washington Post* (Feb. 12, 2014), available at <http://wapo.st/McG3TZ>.

<sup>23</sup> Chris Brummit, *Vietnam’s ‘cyber troops’ take fight to U.S., France*, *Associated Press* (Jan. 20, 2014), available at <http://bit.ly/1uVl4mR>.

<sup>24</sup> Jeremy Wagstaff, *Journalists, media under attack from hackers: Google researchers*, *Reuters* (Mar. 28, 2014), available at <http://reut.rs/1l9SpbW>.

certain outrage in the United States – and rightly so. The U.S. government has already expressed its anger at attempts by foreign governments to reach into the electronic files of United States companies; in May of this year, the Department of Justice indicted five members of the Chinese military for hacking into six U.S. businesses to steal trade secrets – the “first ever charges against a state actor for this type of hacking.”<sup>25</sup> At the same time, the district court’s opinion would discourage foreign media organizations (including some of the Media Amici) from using U.S.-based service providers, out of concern that the U.S. government would be able to seize electronic files in their home countries without complying with local law.

*Second*, the district court’s holding places a further chill on the ability to gather news from whistleblowers and confidential sources. Revelations of government surveillance – both domestically and abroad – have already

---

<sup>25</sup> Dep’t of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014, available at <http://1.usa.gov/1pySTOP>. On a recent visit to Beijing, President Obama urged the Chinese government to halt its cyberattacks. See Cory Bennett, *Obama urges China to stop cyber theft*, The Hill (Nov. 10, 2014), available at <http://bit.ly/1w8KAM1>; Suman Varandani, *U.S. Refuses to ‘Stand Idle’ in Charging China Over Government-Backed Cyberattacks*, International Business Times (Nov. 11, 2014), available at <http://bit.ly/1vF7GqS>.



made sources afraid to contact members of the press, for fear that they will be exposed and prosecuted. AP President Gary Pruitt noted that the revelation that the government had secretly subpoenaed AP phone records cast a chill over not just AP, but other media outlets as well: "Already, officials that would normally talk to us and people we talk to in the normal course of news gathering are already saying to us that they're a little reluctant to talk to us. ... It's not hypothetical. We're actually seeing impact already."<sup>26</sup> Washington Post national security reporter Dana Priest noted: "People think they're looking at reporters' records. I'm writing fewer things in e-mail."<sup>27</sup> New York Times reporter James Risen described a recent encounter where he frightened a source simply by knocking on his front door; terrified of being seen with a reporter, the man "turned white" and hurried him out a back exit.<sup>28</sup>

---

<sup>26</sup> Dylan Byers, *Reporters Say There's a Chill in the Air*, Politico (June 8, 2013), available at <http://politi.co/1AFcj8N>.

<sup>27</sup> Leonard Downie Jr. and Sara Rafsky, *The Obama Administration and the Press*, Committee to Protect Journalists (Oct. 10, 2013), available at <http://bit.ly/1dZ4w5P> (detailing concerns).

<sup>28</sup> Michael Tarm, *Journalists criticize White House for 'secrecy'*, Associated Press (Sept. 17, 2014), available at <http://bit.ly/1uWA7Pw>.

Recently, the ACLU and Human Rights Watch released a report about the chilling effect of U.S. surveillance revelations on journalists' ability to gather and confirm information from increasingly skittish sources. Based on numerous interviews, the authors note:

Journalists repeatedly told us that surveillance had made sources much more fearful of talking. ... [S]ources are "afraid of the entire weight of the federal government coming down on them." Jane Mayer, an award-winning staff writer for *The New Yorker*, noted, "[t]he added layer of fear makes it so much harder. I can't count the number of people afraid of the legal implications [of speaking to me]." One journalist in Washington, DC, noted, "I think many sources assume I'm spied on. [I'm] not sure they're right but I can't do anything about their presumption." As a result, she said, some remaining sources have started visiting her house to speak with her because they are too fearful to come to her office.

*With Liberty to Monitor All: How Large-Scale U.S. Surveillance Is Harming Journalism, Law, and American Democracy*, Human Rights Watch/ACLU (July 2014), at 28, available at <http://bit.ly/1zphRk6>. This culture of fear and silence is only exacerbated by the district court's order allowing U.S. government officials to reach across sovereign borders, without notice to the subscriber, and to gather up the entirety of an email account wherever it is in the world.

## CONCLUSION

For the reasons set forth above, Media Amici respectfully ask this Court to reverse the district court's decision.

Dated: December 15, 2014

Respectfully submitted,

DAVIS WRIGHT TREMAINE LLP

By: s/ Laura R. Handman

Laura R. Handman

Alison Schary

1919 Pennsylvania Avenue, NW

Washington, DC 20006

Tel: (202) 973-4200

Fax: (202) 973-4499

*Attorneys for Media Amici*

### CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,677 words, excluding exempted parts, as determined by the word-counting feature of Microsoft Word.

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Book Antiqua font.

Dated: December 15, 2014

By: s/ Laura R. Handman  
Laura R. Handman

**ADDENDUM:**

**DESCRIPTIONS OF AMICI CURIAE**

**ABC, Inc.** is a broad-based communications company with significant holdings in the United States and abroad. Alone or through its subsidiaries, it owns ABC News, abcnews.com, and local broadcast television stations, including WABC-TV in New York, that regularly gather and report news to the public. ABC News produces the television programs *World News*, *20/20*, *This Week*, *Good Morning America* and *Nightline*, among others.

**Advance Publications, Inc.**, directly and through its subsidiaries, publishes more than 20 print and digital magazines with nationwide circulation, local news in print and online in 10 states, and leading business journals in over 40 cities throughout the United States. Through its subsidiaries, Advance also owns numerous digital video channels and internet sites and has interests in cable systems serving more than 2.3 million subscribers.

With some 500 members, **The American Society of News Editors** (ASNE) is an organization that includes directing editors of daily

newspapers throughout the Americas. ASNE changed its name in April 2009 to the American Society of News Editors and approved broadening its membership to editors of online news providers and academic leaders. Founded in 1922, as the American Society of Newspaper Editors, ASNE is active in a number of areas of interest to top editors with priorities on improving freedom of information, diversity, readership and credibility of newspapers.

The **Association of Alternative Newsmedia** ("AAN") was founded in 1978 and has grown to include 117 alternative news organizations covering every major metropolitan area and other less-populated regions of North America. AAN member publications reach more than 25 million active, educated and influential adults in print, on the web and on mobile devices. The association's members share a strong focus on local news, culture and the arts; an informal style; an emphasis on point-of-view reporting and narrative journalism; a tolerance for individual freedoms and social differences; and an eagerness to report on issues and communities that many mainstream media outlets ignore.

**BH Media Group**, a subsidiary of Berkshire Hathaway, owns 30 daily newspapers and related digital news operations located in Alabama,

Florida, Iowa, Nebraska, New Jersey, North Carolina, Oklahoma, South Carolina, Texas and Virginia. The news media properties operated by BH Media Group include the Omaha World-Herald, Richmond Times-Dispatch, and Tulsa World newspapers, and WPLG-TV in Miami, Florida.

**Cable News Network, Inc.** ("CNN"), a division of Turner Broadcasting System, Inc., a Time Warner Company, is the most trusted source for news and information. Its reach extends to nine cable and satellite television networks; one private place-based network; two radio networks; wireless devices around the world; CNN Digital Network, the No. 1 network of news web sites in the United States; CNN Newsource, the world's most extensively syndicated news service; and strategic international partnerships within both television and the digital media.

**The Daily Beast Company LLC** was founded in 2008 as the vision of Tina Brown and IAC Chairman Barry Diller. Curated to avoid information overload, the site is dedicated to breaking news and sharp commentary. The Daily Beast is the winner of two Webby awards for "Best News" site and regularly attracts more than 18 million unique online visitors a month.

**Daily News, L.P.** publishes the New York Daily News, a daily newspaper that is the seventh-largest paper in the country by circulation.

The Daily News' web site, nydailynews.com, receives approximately 31 million unique visitors each month.

The **European Publishers Council** is a high-level group of 26 Chairmen and CEOs of leading European news media corporations actively involved in multimedia markets with print and digital newspapers, magazines, books journals and database publishers, radio and TV broadcasting, available across all platforms and devices.

The **E.W. Scripps Company** is a diverse, 131-year-old media enterprise with interests in television stations, newspapers, and local news and information web sites. The company's portfolio of locally focused media properties includes: 21 TV stations (11 ABC affiliates, three NBC affiliates, two independents and five Azteca Spanish language stations); daily and community newspapers in 13 markets; and the Washington, D.C.-based Scripps Media Center, home of the Scripps Howard News Service.

**First Look Media, Inc.** is a new non-profit digital media venture that produces The Intercept, a digital magazine focused on national security reporting.



**Fox News Network LLC** owns and operates the number-one rated national cable news network, the Fox News Channel, along with the Fox Business Network, Foxnews.com, Foxbusiness.com, the Fox News Edge, and the Fox News Radio Network.

**Forbes Media** is a global media, branding and technology company, with a focus on news and information about business, investing, technology, entrepreneurship, leadership and affluent lifestyles. The company publishes Forbes, Forbes Asia, Forbes Europe and ForbesLife magazines, as well as Forbes.com and ForbesLife.com. The Forbes brand today reaches more than 75 million people worldwide with its business message each month through its magazines and 36 licensed local editions around the globe, Forbes.com, TV, conferences, research, social and mobile platforms. The Forbes magazine iPad app merges print storytelling with social sharing and the web. Forbes Media's brand extensions include conferences, real estate, education, financial services, and technology license agreements.

**Gannett Co., Inc.** is an international news and information company that publishes 82 daily newspapers in the United States, including USA TODAY, as well as hundreds of non-daily publications. In broadcasting,

the company operates 23 television stations in the U.S. with a market reach of more than 21 million households. Each of Gannett's daily newspapers and TV stations operates internet sites offering news and advertising that is customized for the market served and integrated with its publishing or broadcasting operations.

**Guardian News & Media** (GNM) publishes theguardian.com, the third largest English-speaking newspaper website in the world (comScore, March 2014). Since launching its U.S. and Australia digital editions in 2011 and 2013 respectively, traffic from outside of the U.K. now represents around two-thirds of the Guardian's total digital audience. In the U.K., GNM publishes the Guardian newspaper six days a week, first published in 1821, and the world's oldest Sunday newspaper, The Observer. The Guardian is most recently renowned for its Pulitzer Prize-winning revelations based on the disclosures made by whistleblower Edward Snowden. In 2014, the Guardian was named newspaper and website of the year at the Society of Editors U.K. Press Awards. The Guardian is also known for its globally acclaimed investigation into phone hacking, the launch of its groundbreaking digital-first strategy in 2011 and its trailblazing partnership with WikiLeaks in 2010.

**Hearst Corporation** is one of the nation's largest diversified media companies. Its major interests include the following: ownership of 15 daily and 38 weekly newspapers, including the Houston Chronicle, San Francisco Chronicle and Albany (N.Y.) Times Union; nearly 300 magazines around the world, including Good Housekeeping, Cosmopolitan and O, The Oprah Magazine; 29 television stations, which reach a combined 18 percent of U.S. viewers; ownership in leading cable networks, including Lifetime, A&E and ESPN; business publishing, including a joint venture interest in Fitch Ratings; and internet businesses, television production, newspaper features distribution and real estate.

**The McClatchy Company**, through its affiliates, publishes 28 daily newspapers and related websites, as well as numerous community newspapers and niche publications across the United States.

**MPA - the Association of Magazine Media** is a national trade association including in its present membership more than 240 domestic magazine publishers that publish over 1,400 magazines sold at newsstands and by subscription. MPA members provide broad coverage of domestic and international news in weekly and biweekly publications, and publish weekly, biweekly and monthly publications covering consumer affairs,

law, literature, religion, political affairs, science, sports, agriculture, industry and many other interests, avocations and pastimes of the American people. MPA has a long and distinguished record of activity in defense of the First Amendment.

**The National Press Club** is a membership organization dedicated to promoting excellence in journalism and protecting the First Amendment guarantees of freedom of speech and of press. Founded in 1908, it is the nation's largest journalism association.

**The National Press Photographers Association** ("NPPA") is a 501(c)(6) nonprofit organization dedicated to the advancement of visual journalism in its creation, editing and distribution. NPPA's almost 7,000 members include television and still photographers, editors, students and representatives of businesses that serve the photojournalism industry. Since its founding in 1946, the NPPA has vigorously promoted the constitutional rights of journalists as well as freedom of the press in all its forms, especially as it relates to photojournalism.

**National Public Radio, Inc.** ("NPR") is a District of Columbia nonprofit membership corporation. It produces and distributes its radio programming through, and provides trade association services to, nearly

800 public radio member stations located throughout the United States and in many U.S. territories. NPR's award-winning programs include Morning Edition, and All Things Considered, and serve a growing broadcast audience of over 23 million Americans weekly. NPR also distributes its broadcast programming online, in foreign countries, through satellite, and to U.S. Military installations via the American Forces Radio and Television Service.

**Newspaper Association of America ("NAA")** is a nonprofit organization representing the interests of more than 2,000 newspapers in the United States and Canada. NAA members account for nearly 90 percent of the daily newspaper circulation in the United States and a wide range of non-daily newspapers. The Association focuses on the major issues that affect today's newspaper industry, including protecting the ability of the media to provide the public with news and information on matters of public concern.

The **Online News Association ("ONA")** is the nation's premier organization of digital journalists. ONA's members include reporters, news writers, editors, producers, designers, photographers and others who produce news for distribution over the internet and through other digital

media, as well as academics and others interested in the development of online journalism. ONA is dedicated to advancing the interests of online journalists and the public, generally, by encouraging editorial integrity, editorial independence, journalistic excellence, freedom of expression, and freedom of access.

**PEN American Center, Inc.** ("PEN") is a non-profit association of writers that includes poets, playwrights, essayists, novelists, editors, screenwriters, journalists, literary agents, and translators. PEN has approximately 3,600 members and is affiliated with PEN International, the global writers' organization with 145 centers in more than 100 countries in Europe, Asia, Africa, Australia, and the Americas. Today, PEN works along with the other chapters of PEN International to defend writers and freedom of expression around the world.

**The Reporters Committee for Freedom of the Press** is a voluntary, unincorporated association of reporters and editors that works to defend the First Amendment rights and freedom of information interests of the news media. The Reporters Committee has provided representation, guidance and research in First Amendment and Freedom of Information Act litigation since 1970.

**Seattle Times Company** publishes four newspapers in the State of Washington: The Seattle Times, Washington's most widely circulated daily newspaper; the Yakima Herald-Republic; the Walla Walla Union Bulletin; and The Issaquah Press. Seattle Times Company has been family owned since 1996.

**Tribune Publishing, Inc.** ("Tribune") is one of the country's leading publishing companies. Tribune's leading daily newspapers include the Chicago Tribune, the Los Angeles Times, The Baltimore Sun, the Sun-Sentinel (South Florida), the Orlando Sentinel, the Hartford Courant, The Morning Call, and the Daily Press.

**Verband Deutscher Zeitschriftenverleger ("VDZ")** is the umbrella organization of the German Magazine Publishers Association, an organization of 400 publishers producing more than 3,000 titles in print and digital. VDZ represents 90 percent of the German magazine publishing market.

WP Company LLC (d/b/a **The Washington Post**) publishes one of the nation's most prominent daily newspapers, as well as a website, [www.washingtonpost.com](http://www.washingtonpost.com), that is read by an average of more than 20 million unique visitors per month.

**CERTIFICATE OF SERVICE & CM/ECF FILING**

**14-2985-cv**

I hereby certify that the foregoing Brief of *Amici Curiae* Media Organizations in Support of Appellant was served on all counsel via Electronic Mail generated by the Court's electronic filing system (CM/ECF) with a Notice of Docket Activity pursuant to Local Appellate Rule 25.1.

I also certify that an electronic copy was uploaded to the Court's electronic filing system. Six hard copies of the foregoing Brief of *Amici Curiae* Media Organizations in Support of Appellant were sent to the Clerk's Office by hand delivery to:

Clerk of Court  
United States Court of Appeals, Second Circuit  
Thurgood Marshall U.S. Courthouse  
40 Foley Square  
New York, New York 10007  
(212) 857-8500

on this 15th day of December 2014.

/s/ Samantha Collins  
Samantha Collins