

CAL. NO. \_\_\_\_\_

New York County Criminal Court Clerk's Index No. 2011NY080152

---

**New York Supreme Court**  
APPELLATE TERM—FIRST DEPARTMENT

---

The People of the State of New York,  
*Plaintiffs-Appellees,*

v.

Malcolm Harris,  
*Defendant,*

Twitter, Inc.,  
*Non-Party Movant-Appellant.*

---

**AMICUS CURIAE BRIEF OF AMERICAN CIVIL LIBERTIES UNION,  
NEW YORK CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER  
FOUNDATION, AND PUBLIC CITIZEN, INC.,  
IN SUPPORT OF TWITTER, INC.'S APPEAL**

---

Aden J. Fine  
American Civil Liberties Union  
Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
Telephone: (212) 549-2693

Mariko Hirose  
Arthur Eisenberg  
New York Civil Liberties Union Foundation  
125 Broad Street, 19th Floor  
New York, New York 10004  
Telephone: (212) 607-3300

Marcia Hofmann  
Hanni Fakhoury  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: (415) 436-9333 x. 116

Paul Alan Levy  
Public Citizen Litigation Group  
1600 20th Street, NW  
Washington, D.C. 20009  
Telephone: (202) 588-1000

*Attorneys for Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES ..... i

INTRODUCTION ..... 1

STATEMENT OF INTEREST OF *AMICI CURIAE* ..... 2

FACTUAL AND PROCEDURAL BACKGROUND..... 3

    A. Twitter..... 3

    B. The D.A.’s Subpoena To Twitter..... 6

    C. Procedural Background..... 7

ARGUMENT ..... 8

    I. HARRIS HAS STANDING TO MOVE TO QUASH THE THIRD-PARTY SUBPOENA  
    BECAUSE IT IMPLICATES HIS CONSTITUTIONAL RIGHTS. .... 8

        A. Twitter Users Have Standing To Challenge Third-Party Disclosure Requests That  
        Implicate Their Constitutional Rights..... 9

        B. The Twitter Subpoena Implicates Harris’s First Amendment Rights..... 14

    II. THE TWITTER SUBPOENA VIOLATES THE FIRST AMENDMENT AND ARTICLE  
    I, SECTION 8 OF THE NEW YORK CONSTITUTION..... 23

    III. THE TWITTER SUBPOENA VIOLATES THE FOURTH AMENDMENT AND  
    ARTICLE I, SECTION 12 OF THE NEW YORK CONSTITUTION..... 27

        A. Individuals Have A Reasonable Expectation Of Privacy In Their Locations And  
        Movements Over Time. .... 27

        B. Harris’s Reasonable Expectation Of Privacy Is Not Eliminated Simply Because His IP  
        Addresses Are In The Possession Of Twitter. .... 30

CONCLUSION..... 36

**TABLE OF AUTHORITIES**

**Cases**

*Amazon.com L.L.C. v. Lay*, 758 F. Supp. 2d 1154 (W.D. Wash. 2010) ..... 11, 22, 24, 26

*Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010) ..... 13

*Ashcroft v. ACLU*, 542 U.S. 656, 660 (2004) ..... 26

*Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963)..... 19

*Bradosky v Volkswagen of Am., Inc.*, No. M8-85 (SWK), 1988 WL 5433 (S.D.N.Y. Jan. 15, 1988) ..... 26

*Brock v. Local 375, Plumbers Int’l Union of Am.*, 860 F.2d 346 (9th Cir. 1988) ..... 11

*City of Ladue v. Gilleo*, 512 U.S. 43 (1994) ..... 18

*Cohen v. Google, Inc.*, 887 N.Y.S.2d 424 [Sup Ct, New York County 2009] ..... 13

*Comty.-Serv. Broad. of Mid-Am., Inc. v. FCC*, 593 F.2d 1102 (D.C. Cir. 1978) ..... 17

*Doe v. 2theMart.com, Inc.*, 140 F. Supp. 2d 1088, 1097 (W.D. Wash. 2001)..... 22

*Doe v. Ashcroft*, 334 F. Supp. 2d 471, 508-09 (S.D.N.Y. 2004) ..... 12

*Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) ..... 12

*Doe v. SEC*, No. C 11-80209 CRB, 2011 WL 5600513 (N.D. Cal. Nov. 17, 2011) ..... 11, 12

*Eastland v. U.S. Servicemen’s Fund*, 421 U.S. 491 (1975) ..... 10, 13

*Ex parte Jackson*, 96 U.S. 727, 733 (1877) ..... 33

*Galvin v. Hay*, 374 F.3d 739, 750 (9th Cir. 2004) ..... 18

*Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539 (1963) ..... 15, 23, 24

*Grandbouche v. United States (In re First Nat’l Bank)*, 701 F.2d 115 (10th Cir. 1983)..... 11, 12

*Gravel v. United States*, 408 U.S. 606 (1972) ..... 9

*Greenbaum v. Google, Inc.*, 845 N.Y.S.2d 695 [Sup Ct, New York County 2007]..... 13, 14

*Healy v. James*, 408 U.S. 169, 183 (1972) ..... 19

*In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, No. 10 MC 0897, 2010 WL 5437209, at \*3 (E.D.N.Y. Dec. 23, 2010) ..... 33

<i>In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to Gov’t</i> , 620 F.3d 304 (3d Cir. 2010).....	3, 31
<i>In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)</i> , Misc. No. 1:11-DM-3, 2011 WL 5508991 (E.D. Va. Nov. 10, 2011).....	29
<i>In re Grand Jury Proceeding</i> , 842 F.2d 1229 (11th Cir. 1988).....	11
<i>In re Grand Jury Subpoena Dated Dec. 17, 1996</i> , 148 F.3d 487 (5th Cir. 1998) .....	10, 11
<i>In re Grand Jury Subpoena No. 11116275</i> , Misc. No. 11-527 (RCC), 2012 WL 691599 (D.D.C. Feb. 23, 2012) .....	11
<i>In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006</i> , 246 F.R.D. 570 (W.D. Wis. 2007) .....	21, 23
<i>In re Grand Jury Subpoena</i> , 829 F.2d 1291 (4th Cir. 1987) .....	25
<i>In re Grand Jury</i> , 111 F.3d 1066 (3d Cir. 1997) .....	11, 14
<i>In re Shapiro v Chase Manhattan Bank, N.A.</i> , 84 Misc. 2d 938 [Sup Ct, New York County 1975] .....	13
<i>In re U.S. for an Order Authorizing Installation &amp; Use of a Pen Register &amp; a Caller ID Sys. on Tel. Nos.</i> , 402 F. Supp. 2d 597, 605 n.12 (D. Md. 2005).....	32
<i>In re U.S. for an Order Authorizing the Release of Historical Cell-Site</i> , 809 F.Supp.2d 113 (E.D.N.Y. 2011).....	29, 32, 33
<i>In re U.S. for Historical Cell Site Data</i> , 747 F. Supp. 2d 827 (S.D.Tex. 2010).....	29, 31
<i>In re Verizon Internet Servs., Inc.</i> , 257 F. Supp. 2d 244 (D.D.C. 2003), <i>reversed on other grounds</i> , <i>RIAA v. Verizon Internet Servs., Inc.</i> , 351 F.3d 1229 (D.C. Cir. 2003) .....	14
<i>Katz v. United States</i> , 389 U.S. 347, 352 (1967) .....	33
<i>Kyllo v. United States</i> , 533 U.S. 27 at 34 (2001) .....	34
<i>Lamont v. Postmaster General</i> , 381 U.S. 301 (1965).....	20
<i>Local 1814, Int’l Longshoremen’s Ass’n, AFL-CIO v. Waterfront Comm’n of N.Y. Harbor</i> , 667 F.2d 267 (2d Cir. 1981) .....	10, 12, 25
<i>Mandel v. Bradley</i> , 432 U.S. 173 (1977) ( <i>per curiam</i> ).....	10
<i>McIntyre v. Ohio Elections Comm’n</i> , 514 U.S. 334 (1995).....	16, 22
<i>McVicker v. King</i> , 266 F.R.D. 92 (W.D. Pa. 2010) .....	14

<i>N.Y. Times Co. v. Jasclevich</i> , 439 U.S. 1331 (1978) .....	26
<i>N.Y. Times Co. v. Sullivan</i> , 376 U.S. 254 (1964).....	20
<i>New Jersey v. Reid</i> , 194 N.J. 386, 399-400 (2008).....	36
<i>People ex rel. Arcara v. Cloud Books, Inc.</i> , 68 N.Y.2d 553, 558 (1986) .....	15
<i>People v Di Raffaele</i> , 55 N.Y.2d 234 (1984).....	31
<i>People v. Collier</i> , 376 N.Y.S.2d 954, 979 (Sup. Ct. N.Y. County 1975) .....	16, 20, 23
<i>People v. Hall</i> , 86 A.D.3d 450 [1st Dept 2011].....	29
<i>People v. Laws</i> , 623 N.Y.S.2d 216 [1st Dept. 1995] .....	9
<i>People v. P.J. Video</i> , 68 N.Y.2d 296, 304-05 (1986) .....	35
<i>People v. Weaver</i> , 12 N.Y.3d 433 [2009].....	passim
<i>Perlman v. United States</i> , 247 U.S. 7 (1918).....	10
<i>Pollard v. Roberts</i> , 283 F. Supp. 248 (E.D. Ark. 1968) (three-judge court), <i>aff'd per curiam</i> , 393 U.S. 14 (1968).....	10
<i>Pub. Relations Soc’y of Am., Inc. v. Rd. Runner High Speed Online</i> , 799 N.Y.S.2d 847 [Sup. Ct. N.Y. County 2005].....	13
<i>Rakas v. United States</i> , 439 U.S. 128 (1979).....	9
<i>Register.com, Inc. v. Verio, Inc.</i> , 356 F.3d 393 (2d Cir. 2004).....	5, 17
<i>RIAA v. Verizon Internet Servs., Inc.</i> , 351 F.3d 1229 (D.C. Cir. 2003).....	14
<i>Santa Monica Food Not Bombs v. City of Santa Monica</i> , 450 F.3d 1022, 1047-48 (9th Cir. 2006) .....	18
<i>Shelton v. Tucker</i> , 364 U.S. 479 (1960).....	25
<i>Singleton v. Wulff</i> , 428 U.S. 106 (1976) .....	14
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979) .....	31, 32
<i>Sony Music Entm’t Inc. v. Does 1-40</i> , 326 F. Supp. 2d 556 (S.D.N.Y. 2004).....	5, 17
<i>Turner Broad. Sys., Inc. v. F.C.C.</i> , 512 U.S. 622, 641-42 (1994) .....	15
<i>United States v. Bursey</i> , 466 F.2d 1059 (9th Cir. 1972) .....	24, 25

*United States v. Christie*, 624 F.3d 558 (3d Cir. 2010) ..... 29

*United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008)..... 29

*United States v. Jones*, 132 S. Ct. 945 (2012)..... passim

*United States v. Karo*, 468 U.S. 705, 714-15 (1984)..... 27

*United States v. Miller*, 425 U.S. 435 (1976)..... 12, 31

*United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008) ..... 29

*United States v. Rumely*, 345 U.S. 41 (1953)..... 15

*United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)..... 3, 33, 34

*Velsicol Chem. Corp. v. Parsons*, 561 F.2d 671 (7th Cir. 1977) ..... 11

*Warth v. Seldin*, 422 U.S. 490 (1975)..... 9, 15

**Other Authorities**

Aaron Smith and Joanna Brenner, *Twitter Use 2012*, Pew Internet & American Life Project (May 2012), <http://pewinternet.org/Reports/2012/Twitter-Use-2012.aspx>..... 4

Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 586 (2011) .. 36, 38

Neil MacFarquhar, *Twitter and Facebook are Backbone of Saudi Dissent*, N.Y. Times, June 15, 2011, at A6, available at <http://www.nytimes.com/2011/06/16/world/middleeast/16saudi.html> ..... 4

Stephen E. Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information From Unreasonable Search*, 55 Cath. U. L. Rev. 373, 412 (2006) ..... 38

*Top 500 Global Sites*, Alexa, <http://www.alexa.com/topsites> (last visited Aug. 22, 2012); ..... 4

*Twitter Reaches 500 Million User Mark*, Washington Post, July 30, 2012, ..... 4

## INTRODUCTION

This case arises out of the New York County District Attorney's attempt to subpoena from Twitter more than three months of information about the communications, locations, and movements of Malcolm Harris, an avid Twitter user who is being prosecuted for disorderly conduct in connection with an Occupy Wall Street protest. The D.A.'s subpoena seeks "[a]ny and all user information" and "all tweets," which encompasses not only the content of Harris's tweets, but his personal email address and the date, time, and Internet Protocol address corresponding to each time Harris logged in to his Twitter account over the three-and-a-half month period, regardless of whether he posted any tweets during those times or whether any of his tweets were related to the D.A.'s pending prosecution. The D.A.'s attempt to obtain all of this information through a subpoena, without first obtaining a warrant, violates Harris's First and Fourth Amendment rights, as well as his corresponding rights under the New York Constitution.

The lower court's denial of the motions of Twitter and Harris to quash the subpoena failed to recognize the First Amendment interests implicated by the overbroad subpoena or the Fourth Amendment interests implicated by the demand for the non-public location and movement information that can be derived from Harris's Internet Protocol addresses. Indeed, despite the fact that the subpoena directly targets Harris's speech on Twitter, the court's decision does not address any of the First Amendment issues raised by the subpoena. Equally troubling, the court held that Harris—and by implication, the hundreds of thousands of other Twitter users residing in New York—does not even have standing to challenge the subpoena because it is issued to a third party, Twitter, not to Harris. That holding is at odds with numerous decisions from the United States Supreme Court and lower courts around the country that make clear that individuals whose First Amendment rights are implicated by government requests for

information to third parties have standing to bring motions to quash those third-party requests before their information is disclosed, even if their constitutional challenges are ultimately not successful on the merits. A rule that individuals lose all constitutional protection in information disclosed to third parties would have a devastating effect on free speech and privacy rights, particularly in the digital age where many intimate details of our lives—our thoughts, our movements, our communications, our shopping and browsing habits—are stored by third-party Internet service providers.

*Amici Curiae* the American Civil Liberties Union, the New York Civil Liberties Union, the Electronic Frontier Foundation, and Public Citizen (collectively, “*Amici*”) respectfully submit this memorandum to bring these standing cases to the Court’s attention and to urge the Court to ensure that detailed information concerning individuals’ Internet communications and their locations and movements over time cannot be obtained by the government without first obtaining a warrant and satisfying First and Fourth Amendment scrutiny.

#### **STATEMENT OF INTEREST OF *AMICI CURIAE***

The American Civil Liberties Union (the “ACLU”) is a nationwide, nonprofit, nonpartisan organization with over 500,000 members, dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The New York Civil Liberties Union is the ACLU’s New York affiliate. Founded in 1920, the ACLU has vigorously defended free speech and privacy rights for over ninety years in state and federal courts, in New York and across the country, to protect the constitutional guarantees afforded to free expression and privacy by the U.S. Constitution and the New York Constitution. The ACLU has also been at the forefront of efforts to ensure that the Internet remains a free and open forum for the



exchange of information and ideas and to ensure that the right to privacy remains robust in the face of new technologies.

The Electronic Frontier Foundation (“EFF”) is a non-profit, member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology. As part of that mission, EFF has served as counsel or *amicus curiae* in many cases addressing civil liberties issues raised by emerging technologies. See *United States v. Jones*, 132 S. Ct. 945 (2012); *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *In re Application of U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to Gov’t*, 620 F.3d 304 (3d Cir. 2010).

Public Citizen, Inc., is a public interest organization based in Washington, D.C. It has more than 300,000 members and supporters. Since its founding in 1971, Public Citizen has encouraged public participation in civic affairs, and has brought and defended numerous cases involving the First Amendment rights of citizens who participate in civic affairs and public debates. See generally <http://www.citizen.org/litigation/briefs/internet.htm>. In particular, over the past twelve years, Public Citizen has represented Doe defendants or Internet forum hosts or appeared as *amicus curiae* in cases in which subpoenas have sought to identify hundreds of authors of anonymous Internet messages.

## **FACTUAL AND PROCEDURAL BACKGROUND**

### **A. Twitter.**

Twitter is an Internet service that permits individuals to express their thoughts, views, and opinions with other people around the world, on any subject, in messages of 140 characters or less. Twitter is one of the fastest growing forms of communication in the world, with over

500 million reported registered users as of July 2012, including individuals, corporations, governmental entities, and elected officials.<sup>1</sup> By some estimates it is the ninth largest website in the world.<sup>2</sup> It has become a ubiquitous medium for disseminating the news, organizing protests, opining on current affairs, or simply uttering one's thoughts of the moment. Twitter has been an especially vital form of communication for individuals who either do not have means of access to more traditional media or who live in repressive societies where freedom of speech is not protected, most recently in Syria, Egypt, and Saudi Arabia.<sup>3</sup>

To publish material on Twitter, an individual needs to sign up for a Twitter account. Once that account is opened, a subscriber can publish messages using the account ("tweets"), sign up to receive others' tweets (those one is "following"), and have others follow his or her tweets (one's "followers"). By default, tweets are publicly available. Twitter users have the ability later to delete tweets that they previously posted. Tweets also become no longer visible to the public once a certain number of tweets have been made from an account.

In addition to the contents of a tweet, the time and date of each tweet also appears publicly. The location from where the tweet was made, however, is not publicly available by default. In addition to public tweets, Twitter users may also use Twitter to communicate privately with other Twitter users via Twitter's "Direct Messages" feature, which is the functional equivalent of a private email message service. All information regarding direct

---

<sup>1</sup> *Twitter Reaches 500 Million User Mark*, Washington Post, July 30, 2012, [http://www.washingtonpost.com/business/technology/twitter-reaches-500-million-active-users-140-million-in-the-us/2012/07/30/gJQAVdIMLX\\_story.html?Post+generic=%3Ftid%3Dsm\\_twitter\\_washingtonpost](http://www.washingtonpost.com/business/technology/twitter-reaches-500-million-active-users-140-million-in-the-us/2012/07/30/gJQAVdIMLX_story.html?Post+generic=%3Ftid%3Dsm_twitter_washingtonpost).

<sup>2</sup> *Top 500 Global Sites*, Alexa, <http://www.alexa.com/topsites> (last visited Aug. 22, 2012); see also Aaron Smith and Joanna Brenner, *Twitter Use 2012*, Pew Internet & American Life Project (May 2012), <http://pewinternet.org/Reports/2012/Twitter-Use-2012.aspx> (15% of adult Internet users use Twitter, as of February 2012).

<sup>4</sup> Neil MacFarquhar, *Social Media Help Keep the Door Open to Sustained Dissent Inside Saudi Arabia*, N.Y. Times, June 15, 2011, <http://www.nytimes.com/2011/06/16/world/middleeast/16saudi.html>.

messages, including their content, their sender and recipient, and their time and date, is not publicly available.

A Twitter user's account will contain additional information that is not public, such as "log session" information—e.g., the date, time, and duration of each session in which a user is logged into Twitter—and the Internet Protocol ("IP") addresses for the computer or device used to access Twitter. An IP address is a unique numerical address that identifies individual computers or other devices as they interact over the Internet, allowing information to be transmitted from one to the other. IP addresses can be used to determine the geographic location of a computer and, thus, its user, when they are connected to the Internet on a specific date and time. As the Second Circuit has explained:

The Internet is comprised of numerous interconnected communications and computer networks connecting a wide range of end-users to each other. Every end-user's computer that is connected to the Internet is assigned a unique Internet Protocol number ("IP address"), such as 123.456.78.90, that identifies its location (*i.e.*, a particular computer-to-network connection) and serves as the routing address for email, pictures, requests to view a web page, and other data sent across the Internet from other end-users.

*Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409 (2d Cir. 2004) (citation omitted); *see also Sony Music Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004) (detailing that IP addresses can be matched with publicly available databases to "indicate the 'likely' locations of the residences or other venues where defendants used their Internet-connected computers").<sup>4</sup>

An IP address is also particularly sensitive information because, to the extent an IP address alone does not reveal physical location, once law enforcement learns a user's IP address, it can easily serve one more subpoena to the Internet Service Provider ("ISP") that has assigned that IP address to a particular subscriber to obtain the user's true identity, home or business

---

<sup>4</sup> The accuracy of IP address geolocation can depend on many factors, including how an ISP has set up its network of servers and whether an Internet user utilizes any tools that allow Internet users to obfuscate their IP addresses.

address, telephone number(s), credit card information, and other sensitive and private information.

**B. The D.A.'s Subpoena To Twitter.**

This matter arises out of the New York County District Attorney's (the "D.A.") prosecution of Malcolm Harris, one of the hundreds of individuals accused of committing disorderly conduct by being on the Brooklyn Bridge during an Occupy Wall Street-related protest in October 2011. In connection with that case, on January 26, 2012, the D.A. issued a broadly worded trial subpoena to Twitter (the "Twitter Subpoena") seeking "[a]ny and all user information, including email address, as well as any and all tweets posted for the period of 9/15/2011-12/31/2011," for the account associated with @destructuremal, which was Harris's account. Ex. A.<sup>5</sup> That request covers not only the subscriber information that Harris submitted when he registered for Twitter, including his personal email address, but also the content of all of his tweets, the date, time, and the IP address that corresponds to each time he used Twitter over the three-and-a-half month period, and the duration of each of Harris's Twitter sessions, regardless of whether he posted any tweets during those log-in sessions and regardless of whether any of his tweets were related to the issues involved in the pending prosecution. The plain terms of the Twitter Subpoena—" [a]ny and all user information"—also appear to encompass information concerning Harris's use of Twitter's direct message feature. Some of the information demanded, like IP addresses, email addresses, and direct message information, was never publicly available; other information, like the content of Harris's tweets from the requested period, was once publicly available via Twitter, but no longer was at the time of the subpoena.

---

<sup>5</sup> A copy of the Twitter Subpoena is attached hereto as Exhibit A.

### **C. Procedural Background.**

The D.A. did not notify Harris of the issuance of the Twitter Subpoena. In fact, without any authority, the D.A. “directed” Twitter not to inform Harris of the existence of the trial subpoena. Ex. A. Harris learned of the Subpoena only because Twitter notified him of it following discussions with the D.A., pursuant to Twitter’s policy of informing its customers of such subpoenas unless it is legally restricted from doing so.

Upon receiving notice, Harris filed a motion to quash the Twitter Subpoena on February 6, 2012. The D.A. filed a brief in opposition, alleging that it needed the requested information to refute Harris’s anticipated trial defense that the police either led or escorted him onto the non-pedestrian part of the Brooklyn Bridge. More specifically, the D.A. asserted that the requested information would establish that Harris is the owner of the @destructuremal Twitter account and that he posted tweets from that account contradicting his anticipated defense on the day of the incident. Aff. in Supp. of People’s Resp. to Def.’s Mot. to Quash, at ¶¶ 9-11.

On April 20, 2012, the lower court denied Harris’s motion, holding that he had no standing to challenge the Twitter Subpoena. Decision and Order at 3-6, April 20, 2012 (“April 20 Order”). The court also proceeded to consider the validity of the Subpoena, concluding that it complied with the Stored Communications Act (the “SCA”), *id.* at 8-10, and *sua sponte* issuing an order pursuant to 18 U.S.C. § 2703(d) requiring Twitter to provide the information requested in the Twitter Subpoena within twenty days of receiving notice of the Order, *id.* at 12.

Harris filed a motion to reargue on April 30, 2012. On May 7, 2012, prior to its compliance deadline, Twitter separately filed its own motion to quash the new § 2703(d) order issued by the lower court. *Amici* subsequently filed an amicus brief with the court.

The lower court issued its decision denying Twitter’s motion on June 30, 2012. In its decision, the court upheld its earlier decision that Harris did not have standing to challenge the Subpoena. As before, the court premised this ruling on its belief that Harris did not have a “proprietary interest” in the information requested from Twitter. Decision and Order at 6, June 30, 2012 (“June 30 Order”). The court also concluded that Harris had no standing because he did not have a reasonable expectation of privacy in his Twitter activities. *Id.* at 6-7. The court did not address the First Amendment issues raised by the Subpoena or its April 20 Order or, as explained below, their impact on the standing analysis.

On the merits, the lower court again held that the disclosure demand did not violate the Fourth Amendment, the Stored Communications Act, or any provision of New York law. With respect to the Fourth Amendment, the court concluded that there was no violation because (1) there is no physical intrusion onto Harris’s property and (2) Harris does not have a reasonable expectation of privacy in his tweets that were “intentionally broadcast to the world.” *Id.* at 7. The court’s analysis did not address whether there is an expectation of privacy concerning the non-public subscriber information requested by the Subpoena. As with its standing analysis, the court did not address whether the Subpoena or its April 20 Order violate Harris’s First Amendment rights.

Twitter timely appealed the court’s decision to this Court.

## **ARGUMENT**

### **I. HARRIS HAS STANDING TO MOVE TO QUASH THE THIRD-PARTY SUBPOENA BECAUSE IT IMPLICATES HIS CONSTITUTIONAL RIGHTS.**

The lower court held that Harris did not have standing to challenge the Twitter Subpoena on the ground that individuals have no privacy interest in information possessed by third parties (in this case, Twitter). April 20 Order at 4-6; June 30 Order at 5-7. That conclusion is at odds

with case law from the United States Supreme Court and numerous lower courts holding that individuals whose constitutional rights are implicated by third-party subpoenas have standing to challenge their validity. Because Harris’s First Amendment rights are implicated by the Twitter Subpoena, he has standing to challenge it, even if this Court ultimately holds that Harris should not prevail on the merits of those claims.<sup>6</sup>

**A. Twitter Users Have Standing To Challenge Third-Party Disclosure Requests That Implicate Their Constitutional Rights.**

“In essence the question of standing is whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.” *Warth v. Seldin*, 422 U.S. 490, 498 (1975). That question “in no way depends on the *merits* of the plaintiff’s contention that particular conduct is illegal.” *Id.* at 500 (emphasis added). In other words, as long as a threshold showing is made that one’s First Amendment rights are in jeopardy, an individual has standing to seek to protect those rights, regardless of the merits of those claims. Because Harris’s First Amendment rights are implicated by the Twitter Subpoena, *see infra* at 14-22, he has standing to challenge its validity, even if the Court subsequently determines on the merits that his rights were not violated in these particular circumstances.

The United States Supreme Court has repeatedly held that individuals whose constitutional rights are implicated by a government subpoena to a third party have standing to challenge the request to attempt to protect their constitutional rights before disclosure of the requested information. *See, e.g., Gravel v. United States*, 408 U.S. 606, 608-09 (1972) (Senator Gravel allowed to intervene to file motion to quash grand jury subpoena issued to third party to

---

<sup>6</sup> This section focuses on Harris’s standing to challenge the subpoena on First Amendment grounds. In the Fourth Amendment context, the separate issues of standing and the merits are more closely related. *Rakas v. Illinois*, 439 U.S. 128, 139-40 (1978); *People v. Laws*, 623 N.Y.S.2d 216, 218 (App. 1st Dep’t. 1995) (stating that the *Rakas* rule applies under the New York Constitution). As a result, rather than separately address Harris’s standing to bring a Fourth Amendment challenge to the Subpoena, *amici* address this issue in the context of discussing the merits of Harris’s Fourth Amendment objections. *See infra* at 27-36.

protect his rights under the Speech and Debate Clause); *Pollard v. Roberts*, 283 F. Supp. 248, 258-59 (E.D. Ark. 1968) (three-judge court), *aff'd per curiam*, 393 U.S. 14 (1968) (considering targets' challenge to subpoenas directed at third-party bank, and enjoining subpoenas because enforcement would violate targets' First Amendment rights);<sup>7</sup> *Perlman v. United States*, 247 U.S. 7, 12-13 (1918) (permitting individual to raise constitutional objections to disclosure of documents in the possession of a third party, and to appeal denial of motion immediately). As the Court explained in *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491 (1975), if individuals about whom information was being sought from a third party were not permitted to bring such an action, their constitutional rights could permanently be frustrated because they could not count on the third party-recipient to stand up for their rights. *Id.* at 501 n.14 (holding that the lower court properly entertained the plaintiffs' challenge of a congressional subpoena issued to their third-party bank); *see also id.* at 514 (Marshall, J., concurring) (emphasizing that before disclosure, the target must be given a forum to "assert its constitutional objections to the subpoena, since a neutral third party could not be expected to resist the subpoena by placing itself in contempt").

Courts around the country have followed suit, holding that individuals whose constitutional rights are implicated by subpoenas to third parties have standing to challenge them, even if the individuals do not presently have a possessory interest in the information sought.<sup>8</sup> That is true even if, as in *Eastland*, the Court ultimately rejects the constitutional challenge on the merits. *Id.* at 507.

---

<sup>7</sup> A *per curiam* affirmation of a three-judge trial court decision by the Supreme Court is a judgment on the merits, preventing "lower courts from coming to opposite conclusions on the precise issues presented and necessarily decided by those actions." *See, e.g., Mandel v. Bradley*, 432 U.S. 173, 176 (1977) (*per curiam*).

<sup>8</sup> *See, e.g., Local 1814, Int'l Longshoremen's Ass'n, AFL-CIO v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 271 (2d Cir. 1981) (permitting a labor union and its political action committee to challenge a subpoena for a third party's business records); *In re Grand Jury Subpoena Dated Dec. 17, 1996*, 148 F.3d 487, 490 (5th Cir. 1998) ("[T]he Government contends that the Moczygembas lacked standing to challenge the grand jury subpoena because



In reaching its initial decision on standing, the lower court relied heavily on Twitter's Terms of Service and its Privacy Policy. April 20 Order at 3, 5. The Terms of Service and the Privacy Policy, like the similar ones of many other Internet companies, do not, however, alter the First Amendment standing analysis here. Indeed, in *In re Grand Jury Subpoena No. 11116275*, 846 F. Supp. 2d 1 (D.D.C. 2012), a federal court recently permitted a Twitter user to bring a motion challenging a grand jury subpoena issued to Twitter for his subscriber information. *Id.* at 7. Another federal court reached the same conclusion with respect to a Google/Gmail user, rejecting the government's argument that the Gmail user had no standing to challenge a subpoena to Google for the user's subscriber information because the user had voluntarily provided that information to Google. *Doe v. SEC*, No. C 11-80209 CRB, 2011 WL 5600513, at \*3 (N.D. Cal. Nov. 17, 2011). Amazon.com customers have similarly been permitted to challenge government demands to Amazon for their account information. *Amazon.com L.L.C. v. Lay*, 758 F. Supp. 2d 1154 (W.D. Wash. 2010).<sup>9</sup>

That the information is in the physical possession of Twitter, a third party, similarly does not eliminate Harris's right to challenge the Twitter Subpoena. *See, e.g., In re Grand Jury Subpoena Dated Dec. 17, 1996*, 148 F.3d at 490 (rejecting a virtually identical argument that the movants lacked standing because they no longer had "a possessory interest in the documents

---

the subpoena was not directed at them, nor did they have a possessory interest in the documents requested. This contention is without merit. A third party has standing to challenge a grand jury subpoena where the third party has a claim of privilege respecting information or materials sought by the subpoena."); *In re Grand Jury*, 111 F.3d 1066, 1073 (3d Cir. 1997) ("The Supreme Court and this court have on several occasions allowed third parties to move to quash grand jury subpoenas directed to others. . . . It is well-established that a litigant may have sufficiently important, legally-cognizable interests in the materials or testimony sought by a grand jury subpoena issued to another person to give the litigant standing to challenge the validity of that subpoena.") (listing and discussing cases); *Brock v. Local 375, Plumbers Int'l Union of Am.*, 860 F.2d 346, 349 (9th Cir. 1988) (same); *In re Grand Jury Proceeding*, 842 F.2d 1229, 1234 (11th Cir. 1988) (same); *Grandbouche v. United States (In re First Nat'l Bank)*, 701 F.2d 115, 117-19 (10th Cir. 1983) (same); *Velsicol Chem. Corp. v. Parsons*, 561 F.2d 671, 674 (7th Cir. 1977) (same).

<sup>9</sup> Twitter users also retain a property interest in their tweets pursuant to Twitter's terms of service, which is an independent basis for sustaining Harris's standing to challenge the Subpoena. Memorandum in Support of Twitter's Motion to Quash at 4.

requested”); *Doe v. SEC*, 2011 WL 5600513, at \*3 (same); *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 508-09 (S.D.N.Y. 2004), *vacated and rev’d on other grounds*, *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006). Indeed, in *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court expressly recognized that First Amendment claims may be implicated by the summons of records held by a third-party bank, even if the Fourth Amendment is not implicated. *Id.* at 444 n.6. “This is so because the constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third parties.” *In re First Nat’l Bank*, 701 F.2d at 118 (rejecting the government’s assertion that the Supreme Court’s decision in *Miller* forecloses petitioners from having standing to challenge a third-party request); *see also Local 1814*, 667 F.2d at 271 (same).

Were it otherwise, Internet users would never have standing to defend their constitutional right to associate or to engage in anonymous speech on the Internet, because users must provide their information to others—e.g., to ISPs—to access the Internet. As Judge Marrero, a federal district judge in the Southern District of New York, explained:

[T]he implications of the Government’s position [that disclosure to third parties eliminates the right to anonymity] are profound. Anonymous internet speakers could be unmasked merely by an administrative, civil, or trial subpoena, or by any state or local disclosure regulation directed at their ISP, and the Government would not have to provide any heightened justification for revealing the speaker. The same would be true for attempts to compile membership lists by seeking the computerized records of an organization which uses a third-party electronic communications provider. Considering, as is undisputed here, the importance of the internet as a forum for speech and association, the Court rejects the invitation to permit the rights of internet anonymity and association to be placed at such grave risk.

*Doe v. Ashcroft*, 334 F. Supp. 2d at 509.

Indeed, state and federal courts around the country, including courts in New York, have consistently permitted Internet users to bring motions to quash third-party subpoenas issued to their third-party ISPs to protect their First Amendment rights, even though the users knowingly provided the requested information to their ISPs. *See, e.g., Pub. Relations Soc’y of Am., Inc. v. Rd. Runner High Speed Online*, 799 N.Y.S.2d 847 [Sup. Ct. N.Y. County 2005] (adjudicating motion to quash subpoena by anonymous Internet user whose identifying information was being sought from ISP); *Cohen v. Google, Inc.*, 887 N.Y.S.2d 424 (Sup. Ct. N.Y. County 2009) (same); *Greenbaum v. Google, Inc.*, 845 N.Y.S.2d 695, 698 (Sup. Ct. N.Y. County 2007) (same); *Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010) (same).

One of the principal rationales behind *Eastland* and all of these other cases is that the individuals whose constitutional rights are implicated by third-party subpoenas must be given an opportunity to challenge them immediately, because the third parties do not have the necessary incentives to do so. *Eastland*, 421 U.S. at 501 n.14; *id.* at 514 (Marshall, J., concurring) (stating that the target must be given a forum to “assert its constitutional objections to the subpoena, since a neutral third party could not be expected to resist the subpoena by placing itself in contempt”); *see also In re Shapiro v. Chase Manhattan Bank, N.A.*, 84 Misc. 2d 938, 943 (Sup. Ct. N.Y. County 1975) (“Banks cannot be expected to resist a subpoena by placing themselves in contempt, and compliance by the third-party bank clearly would frustrate any judicial determination of the issue.”). The same concern exists here.

Although Twitter has filed its own motion in this case, that does not mean that it (or other companies) will do so in other cases. Indeed, its lower court brief makes clear that one of the reasons why Twitter weighed in here is because of the potential consequences for Twitter of the lower court’s holding that the thousands of Twitter users in New York do not have standing to

challenge any governmental requests for information about them. Memorandum in Support of Twitter’s Motion to Quash at 5. The reality is that Twitter, like other companies, will not—and cannot—challenge every government request directed at one of its millions of users, who pay Twitter no money and have no relationship with Twitter other than that they use its services. *Cf. Greenbaum*, 845 N.Y.S.2d at 698 (permitting intervention by user to challenge subpoena to Google because, *inter alia*, “Google leaves it to those people to come in and protect their own interests.” (citation and internal quotation marks omitted)).<sup>10</sup>

Because Twitter and similar entities do not have the incentives to challenge these government requests, Internet users—the individuals whose constitutional rights are at stake—are precisely the people who must have standing to defend those rights in court. *See, e.g., Singleton v. Wulff*, 428 U.S. 106, 113–14 (1976) (holding that individuals whose personal rights are at stake “usually will be the best proponents of their own rights”); *In re Grand Jury*, 111 F.3d 1066, 1072 (3d Cir. 1997) (“Because it is Doe 1 and Doe 2 whose privacy has been violated and would again be violated by compliance with the [grand jury] subpoena . . . it is the intervenors and not the witness herself who are best suited to assert the Title III claim.”). Although the information requested may be in Twitter’s possession, the First Amendment interests at stake belong primarily to Harris, and Harris’s rights are best raised by Harris, not by Twitter.<sup>11</sup>

#### **B. The Twitter Subpoena Implicates Harris’s First Amendment Rights.**

Because, contrary to the lower court’s belief, individuals can have standing to challenge third-party subpoenas, whether Harris has standing here turns on whether his constitutional rights

---

<sup>10</sup> Twitter has standing to raise the constitutional rights of its users, like Harris, if it chooses to do so. *See, e.g., In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 257-58 (D.D.C. 2003), *rev’d on other grounds, RIAA v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003) (holding that Verizon had standing to raise the rights of its ISP customers in challenge to subpoena it received); *McVicker v. King*, 266 F.R.D. 92, 95-96 (W.D. Pa. 2010) (same for newspaper seeking to defend rights of individuals posting comments on its website).

<sup>11</sup> Twitter may also enjoy a First Amendment interest as a platform for speech, but the primary First Amendment interest at issue here is the individual Twitter user’s First Amendment rights.

are implicated by the Twitter Subpoena. Harris need not demonstrate that he can prevail on the merits of his claims for his rights to be implicated; he must simply make a threshold showing that those rights are in jeopardy. *Warth*, 422 U.S. at 500. Harris meets this standard.<sup>12</sup>

At its most elementary level, the First Amendment prohibits government from taking actions that burden speech except in extraordinary circumstances. *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 641-42 (1994). More specifically, courts have recognized that government demands for information concerning expressive activities inherently burden speech and therefore implicate the First Amendment and its New York equivalent, Article I, Section 8. *See, e.g., Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 558 (1963) (“It is particularly important that the exercise of the power of compulsory process be carefully circumscribed when the investigative process tends to impinge upon such highly sensitive areas as freedom of speech or press, freedom of political association [sic], and freedom of communication of ideas.” (citation and internal quotation marks omitted)); *United States v. Rumely*, 345 U.S. 41, 46 (1953) (holding that a subpoena to a bookseller implicated the First Amendment); *People ex rel. Arcara v. Cloud Books, Inc.*, 68 N.Y.2d 553, 558 (1986) (stating that under the New York Constitution, “[t]he crucial factor in determining whether State action affects freedom of expression is the impact of the action on the protected activity and not the nature of the activity which prompted the government to act”).

The Twitter Subpoena seeks “[a]ny and all user information” about Harris’s use of Twitter over a three-and-a-half month period, including the political views and personal opinions that Harris expressed in his tweets and the location of where he was at those times. That type of prolonged, wholesale surveillance into speech activities implicates the First Amendment because

---

<sup>12</sup> The merits of Harris’s First Amendment and Fourth Amendment claims are separately discussed below. *See infra* at 23-36.

“[a]wareness that the Government may be watching chills associational and expressive freedoms.” *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *see also People v. Collier*, 376 N.Y.S.2d 954, 979 (Sup. Ct. N.Y. County 1975) (“We cannot live in a free society where we have a sense of being observed by government watchers. Unwarranted police surveillance will destroy our capacity to tolerate—and even encourage—dissent and nonconformity; it promotes a climate of fear; it intimidates, demoralizes and frightens the community into silence.”). If people know that the government will be monitoring their speech and creating dossiers on their past, present, and future communications such that they will be held accountable for everything that they say, people will be less inclined to speak or read as freely. That is especially the case with respect to “casual,” spontaneous speech, because individuals would likely refrain from publicly making such statements or flipping through random books or websites as often if they thought that the government might later obtain that information and hold it against them.

That the content of Harris’s tweets was once publicly available does not mean that there are no First Amendment issues raised by the Subpoena. The First Amendment protects both public and non-public speech. Indeed, the whole point of the First Amendment is to protect speech made in public that others—namely, the majority—might not like and might not want others to hear. Newspapers, for example, are indisputably protected by the First Amendment, despite their “public” nature. Likewise, in *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334 (1995), the United States Supreme Court made clear that the plaintiff retained her right to refuse to disclose her identity even though she was engaging in her anonymous speech in public, in full view of everyone who could see her and identify her.

The precise scenario at issue here—a demand for disclosure of information about already-published speech—is unusual. But that is only because there is usually no need to subpoena information that is publicly available; here, there is such a need because Harris’s once-public tweets are no longer publicly available. That does not, however, mean that the First Amendment is not triggered. Indeed, in a factually similar context, the D.C. Circuit held that the government’s attempt to force disclosure of already-published content that was once publicly available not only implicated, but violated, the First Amendment because of its impact on the targeted speech. *Comty.-Serv. Broad. of Mid-Am., Inc. v. FCC*, 593 F.2d 1102, 1122 (D.C. Cir. 1978). In that case, the D.C. Circuit invalidated an F.C.C. requirement that government-funded, non-commercial radio stations tape-record all broadcast public affairs programs and later make the recordings available to F.C.C. Commissioners, holding that the requirement was unconstitutional because it was likely to chill free expression and served no legitimate government interest. In other words, just because an individual’s speech activities were once publicly viewable does not mean that there is no First Amendment protection for them.

The government surveillance at issue here is especially concerning because, in addition to demanding the content of Harris’s once-publicly available tweets, the Twitter Subpoena also requests information that was never publicly accessible, such as the IP addresses associated with Harris’s use of Twitter and the date and time for each log-in session. As explained above, IP addresses correlate to a user’s specific geographic location. *Register.com*, 356 F.3d at 409; *Sony Music*, 326 F. Supp. 2d at 567. The linking of Harris’s locations with the content of his messages makes the Twitter Subpoena particularly invasive from a First Amendment perspective because information about Harris’s location may provide meaning to some of his tweets that might not otherwise be apparent to the public. “The [Supreme] Court has recognized that

location of speech, like other aspects of presentation, can affect the meaning of communication and merit First Amendment protection for that reason.” *Galvin v. Hay*, 374 F.3d 739, 750 (9th Cir. 2004) (citing *City of Ladue v. Gilleo*, 512 U.S. 43 (1994)). For example, a message such as “I like the government here” both derives meaning from and conveys meaning about the speaker’s location; it would mean one thing if tweeted from Peoria and quite another if tweeted from Pyongyang. Likewise, tweeting “Everybody must get stoned” might mean one thing if tweeted from Woodstock on the night of a Bob Dylan concert, but something far different if tweeted from Kandahar on a day in which numerous citizens are stoned to death for committing moral offenses. Similarly, “Take the bridge” might mean one thing if tweeted from lower Manhattan on October 1, 2011, and a far different thing if tweeted from near the Golden Gate Bridge on September 11, 2001. Indeed, that is precisely why the D.A. wants to obtain the content of Harris’s tweets; *where* people are when they say certain things matters. *See City of Ladue v. Gilleo*, 512 U.S. 43, 56 (1994) (“Displaying a sign from one’s own residence often carries a message quite distinct from placing the same sign someplace else, or conveying the same text or picture by other means.”); *Santa Monica Food Not Bombs v. City of Santa Monica*, 450 F.3d 1022, 1047-48 (9th Cir. 2006) (“[A] location itself may be significant to the content of the message.”). Connecting Harris’s locations and movements to his specific messages may, thus, provide the D.A. with nuanced insight not just into Harris’s daily life, but his expressive activities as well.

On their own, some of these details about Harris’s communications might not seem terribly invasive. From a First Amendment perspective, however, even small infringements require compelling justification because “[f]reedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental



interference.” *Healy v. James*, 408 U.S. 169, 183 (1972); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963) (“It is characteristic of the freedoms of expression in general that they are vulnerable to gravely damaging yet barely visible encroachments.”).

Moreover, given the amount of time covered by the Subpoena—three-and-a-half months—the accumulation of all of these discrete details and data points from such a long period of time could enable the D.A. to piece together a comprehensive portrait of Harris’s expressive activities and habits, directly implicating his First Amendment rights. *Cf. Jones*, 132 S. Ct. at 955 (Sotomayor, J. concurring) (stating that GPS monitoring “generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations”); *People v. Weaver*, 12 N.Y.3d 433, 442 [2009] (holding that GPS monitoring reveals “a highly detailed profile, not simply of where we go, but by easy inference, of our associations . . . and of the pattern of our professional and avocational pursuits”).<sup>13</sup> Indeed, whereas government monitoring of a single public speech activity might not necessarily trigger First Amendment protections, the government’s ability to amass and maintain a comprehensive database of one’s digital speech activities over a three-and-a-half month period implicates far more serious constitutional concerns, especially, where, as here, technological advances have made it so easy and relatively cost-free for government to do so. *Cf. Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (“[T]he Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom

---

<sup>13</sup> That is especially true for an active Twitter user like Harris. Because Harris published so many tweets each day, and because it is likely that he logged on to Twitter far more often than just when he published his own tweets—e.g., to view others’ tweets—the information the D.A. is demanding will provide a highly detailed, comprehensive index of Harris’s daily communications activities, his locations, and his movements over a prolonged period of time—108 days—regardless of whether they have any connection to the pending disorderly conduct action.

the Government, in its unfettered discretion, chooses to track—may ‘alter the relationship between citizen and government in a way that is inimical to democratic society.’” (internal citation omitted)); *Weaver*, 12 N.Y.3d at 441 (“That such a surrogate technological deployment is not—particularly when placed at the unsupervised discretion of agents of the state ‘engaged in the often competitive enterprise of ferreting out crime’—compatible with any reasonable notion of personal privacy or ordered liberty would appear to us obvious.” (internal citation omitted)).

If individuals knew that the government could combine what they have been saying for the past three-and-a-half months with where they were when they said those things, what time of day they read certain websites or communicated with their friends, how long they read certain websites and took to write messages, and whether communications were made via a mobile phone, laptop, or personal computer (and therefore whether the individuals were more likely to say certain things from work, from their home, or from coffee shops), the certain result would be that individuals would be chilled from engaging in those communications as freely. As a result, the D.A. cannot simply subpoena this information without first satisfying constitutional scrutiny. *See, e.g., Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965) (holding that the forced disclosure of reading habits “is at war with the ‘uninhibited, robust, and wide-open’ debate and discussion that are contemplated by the First Amendment”) (quoting *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)); *Collier*, 376 N.Y.S.2d at 984 (explaining that even small infringements of constitutional rights cannot be permitted).

That is especially true given the nature of the speech at issue—Internet speech. Although the prevalence of the Internet and its accompanying technological advances, such as Twitter, provide invaluable tools for creating and disseminating information, the unprecedented potential for Internet companies to store vast amounts of personal information for an indefinite time—and

for the government to obtain that information—poses a new threat to free speech and the right to personal privacy. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). The ease with which information is spread over the Internet exacerbates the chilling effect that would likely be felt—rationally or otherwise—from broad government surveillance of speech, particularly on such a high-profile and politically charged matter as the Occupy Wall Street protests. As one court explained in considering a grand jury subpoena to Amazon.com:

[I]f word were to spread over the Net—and it would—that [the government] had demanded and received Amazon’s list of customers and their personal purchases, the chilling effect on expressive e-commerce would frost keyboards across America. Fiery rhetoric quickly would follow and the nuances of the subpoena (as actually written and served) would be lost as the cyberdebate roiled itself to a furious boil. One might ask whether this court should concern itself with blogger outrage disproportionate to the government’s actual demand of Amazon. The logical answer is yes, it should: well-founded or not, rumors of an Orwellian federal criminal investigation into the reading habits of Amazon’s customers could frighten countless potential customers into canceling planned online book purchases, now and perhaps forever.

*In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006*, 246 F.R.D. 570, 573 (W.D.

Wis. 2007). Thus, even if the Court believes that individuals *should* not be chilled by the actual language of the Twitter Subpoena or because it concerns already-public communications, countless individuals likely *will be* chilled by the government’s demand for information about individuals’ Internet communications.

Moreover, although the D.A. has now disclaimed any intent to seek information concerning Harris’s use of Twitter’s direct messaging feature, the plain terms of the Twitter Subpoena—“[a]ny and all user information”—appear to encompass that information as well. Because the D.A. has not conceded that the wording of the Twitter Subpoena is improper in any manner and because it has not agreed that it will never ask for the full scope of the originally-demanded information, the Subpoena’s validity turns on its plain language, not on what the D.A.

now claims it intended the Subpoena to cover. *See, e.g., Amazon.com, L.L.C. v. Lay*, 758 F. Supp. 2d 1154, 1169 & n.2 (W.D. Wash. 2010) (rejecting the government’s argument that a document demand should be read to cover only what the government says it intended, instead of the plain language of the demand). Direct messages, like emails or letters, are private and are intended to be seen only by the individuals communicating with each other via direct messages. The content of those direct messages is indisputably constitutionally protected. Disclosure of Harris’s direct messages would also reveal the date, time, and IP address of every individual with whom Harris either sent or received a direct message, providing a detailed dossier on Harris’s friends and associates, as well as on him. Information concerning Harris’s use of direct messages, thus, directly implicates Harris’s First Amendment interests.

Finally, as discussed below, one of the D.A.’s rationales for demanding the requested non-public subscriber information is to ascertain whether Harris was actually the individual who posted the tweets in question. To the extent the identity of the poster of those tweets is unknown, the demand for this identifying information indisputably implicates the First Amendment right to engage in anonymous speech. *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (“[A]nonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.”); *Doe v. 2theMart.com, Inc.*, 140 F. Supp. 2d 1088, 1097 (W.D. Wash. 2001) (“[T]he constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.”).

The lower court did not even attempt to address any of these First Amendment issues. That was error. Because Harris’s First Amendment rights are implicated by the Twitter Subpoena, he has standing to challenge it, regardless of whether he ultimately prevails on the merits of his First Amendment claims.

## II. THE TWITTER SUBPOENA VIOLATES THE FIRST AMENDMENT AND ARTICLE I, SECTION 8 OF THE NEW YORK CONSTITUTION.

Because the Twitter Subpoena and the lower court's orders enforcing it implicate Harris's First Amendment rights, the D.A. must show both an "overriding and compelling" government interest in obtaining the requested information and a substantial nexus between the information and that governmental interest to overcome constitutional scrutiny. *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963) (holding that a state legislative committee subpoena could not be enforced because "it is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech . . . that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest"); *Collier*, 376 N.Y.S.2d at 984 ("When the police unilaterally decide that there is a need to gather data with respect to a person's association with others engaged in lawful political, social or community activity, that agency of government should be prepared to show a substantial relationship between the information sought and some compelling government interest."). The D.A. has not made and cannot make this showing here.

As the lower court noted in its April 20 Order, the D.A. claims that it needs this information (1) to establish that Harris is the owner of the @destructuremal account—*i.e.*, that he is the individual who posted the tweets through that account—and (2) to demonstrate that "while on the Brooklyn Bridge the defendant may have posted Tweets that were inconsistent with his anticipated trial defense." April 20 Order at 11. Because the D.A. cannot establish that it "actually needs the disputed information" to prove either of those points, the Twitter Subpoena cannot pass First Amendment scrutiny. *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. at 572.

First, as far as *amici* are aware, there is no dispute that the account in question is Harris’s Twitter account, and that he is the one who published the tweets on that account. Nor is there any dispute that Harris was in New York and on the Brooklyn Bridge when he was arrested there. Because Harris is not contesting these facts, the D.A. does not need to obtain any subscriber information from Twitter, including his IP addresses or the date, time, and duration of his many Twitter sessions, to prove these facts. At most, all that the D.A. needs—and all that the D.A. should be permitted to obtain, if anything—is information sufficient to show that on the day in question, Harris was the one posting tweets through that account.

Second, to the extent the D.A. wants access to Harris’s tweets from the day in question to establish contradictions with his anticipated trial version of what happened on that day, or to clarify “the contested issue of defendant’s state of mind at the time he chose to defy police orders and block the Brooklyn Bridge,” Aff. in Supp. of People’s Resp. to Def.’s Mot. to Reargue at 7, all the D.A. needs are those specific tweets. The D.A. does not need any information about Harris’s locations and movements or his Twitter activities or tweets for any of the other 107 days—or even tweets from the one day in question that had nothing to do with the Brooklyn Bridge incident—to establish any such contradictions or Harris’s “state of mind.” Because the D.A. cannot establish a substantial nexus between the information requested and the D.A.’s alleged need for the information, the Twitter Subpoena cannot withstand First Amendment scrutiny. *See, e.g., Gibson*, 372 U.S. at 546; *Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972); *Lay*, 758 F. Supp. 2d at 1169 & n.2 (invalidating disclosure demand to Amazon.com because the information requested about Amazon users was not necessary to accomplish North Carolina’s stated goals); *Collier*, 376 N.Y.S.2d at 984.<sup>14</sup>

---

<sup>14</sup> There is also a serious question as to whether the D.A. can even establish that it has a compelling or overriding interest in obtaining the information. Although the D.A. has not expressly articulated its government interest, the

For many of the same reasons, the Twitter Subpoena is also unconstitutional because it is overbroad and impermissibly sweeps in a vast swath of information about Harris’s expressive activities that the D.A. has no legitimate need to know. Where, as here, the government seeks information that is protected by the First Amendment, it “must use a scalpel, not an ax.” *Bursey*, 466 F.2d at 1088; *see also Local 1814*, 667 F.2d at 273 (holding that a third-party subpoena is invalid “when the end can be more narrowly achieved”) (quoting *Shelton v. Tucker*, 364 U.S. 479, 488 (1960) (quotation marks omitted)).

The Twitter Subpoena fails to “use a scalpel” because it broadly seeks “all tweets” and “[a]ny and all user information” for 108 days, even though the D.A. cannot claim that all—or even most—of Harris’s tweets have anything to do with the one-day Brooklyn Bridge incident or Harris’s state of mind at the time of the incident, and even though the D.A. has failed to articulate any reason for needing Harris’s IP addresses or log session information. Moreover, the plain terms of the Subpoena call for the production of “[a]ny and all” information concerning Harris’s use of Twitter’s direct messaging feature, which even the D.A. now concedes it does not need. Because the D.A. could have issued a much narrower subpoena to obtain the information it claims it needs, the Twitter Subpoena is unconstitutional. *See, e.g., In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d 1291, 1302 (4th Cir. 1987) (quashing a subpoena requiring videotape distributors to produce copies of videos, and holding that the government must act “in the least intrusive manner possible, which means, at a minimum, by identifying the requested material in a way that allows the recipient of the subpoena to know immediately

---

D.A. presumably would assert that the information is relevant to the prosecution of Harris and that the prosecution of allegedly unlawful conduct is a compelling government interest. Legitimate as that interest may be, not all legitimate government interests are “compelling” or “overriding” government interests, and there are serious questions as to whether obtaining additional evidence to bolster a prosecution for disorderly conduct—a “violation” that does not even rise to the level of a criminal misdemeanor—can constitute an “overriding and compelling” government interest that is sufficient to justify even a potential infringement of First Amendment rights. The Court need not answer that question here.

whether an item is to be produced or not”); *Lay*, 758 F. Supp. 2d at 1169 (holding that the government’s demand to Amazon.com for “all information as to all sales” was unconstitutionally overbroad because the “requests are not the least restrictive means to obtain the information” needed).

In its April 20 Order, the lower court suggested that any constitutional concerns would be “balanced and protected by the *in camera* review of the materials sought.” April 20 Order at 11. Reiterating that belief, the court has now ordered Twitter to provide the requested information to the court, and stated that the court will then determine which of those materials are relevant and will be disclosed to the D.A. June 30 Order, at 11. Although *in camera* review may minimize some of the harm and may be appropriate in certain circumstances, it is not a cure for the Twitter Subpoena’s constitutional defects because even that review can implicate Harris’s First Amendment interests. See *N.Y. Times Co. v. Jasclevich*, 439 U.S. 1331, 1335-36 (1978) (Marshall, J., in chambers) (holding that forced disclosure even for *in camera* review purposes can inhibit First Amendment rights); *Bradsky v Volkswagen of Am., Inc.*, No. M8-85 (SWK), 1988 WL 5433, at \*3 (S.D.N.Y. Jan. 15, 1988) (stating that an *in camera* inspection “in and of itself impacts on the First Amendment rights” of the entity seeking to prevent disclosure). Critically, even if an *in camera* review were deemed appropriate, the lower court should release information to the D.A. only if the D.A. has first met its constitutional burden with respect to that specific information, not just if the court deems the information to be “relevant” to this case. *Ashcroft v. ACLU*, 542 U.S. 656, 660 (2004) (“the Government bear[s] the burden” of showing the constitutionality of content-based regulations of speech). Because the D.A. has not met that burden here, *in camera* review is not a cure for the Subpoena’s constitutional infirmities.



### **III. THE TWITTER SUBPOENA VIOLATES THE FOURTH AMENDMENT AND ARTICLE I, SECTION 12 OF THE NEW YORK CONSTITUTION.**

The Twitter Subpoena also implicates Harris’s fundamental rights under the Fourth Amendment and Article I, Section 12 of the New York Constitution. Absent exigent or other exceptional circumstances, the Fourth Amendment and its state-law counterpart require the government to obtain a warrant supported by probable cause when it intrudes on reasonable expectations of privacy. *See Weaver*, 12 N.Y.3d at 439, 444. Here, the D.A. is attempting to access a wealth of personal information—a database of Harris’s historical speech activities and corresponding IP addresses that are, contrary to the lower court’s decision, not visible to the public—without a warrant, through a mere subpoena. Because this non-public information would reveal Harris’s locations and movements over a three-and-a-half month period, the Subpoena infringes his reasonable expectation of privacy.

#### **A. Individuals Have A Reasonable Expectation Of Privacy In Their Locations And Movements Over Time.#**

In *People v. Weaver*, the New York Court of Appeals held that people have reasonable expectations of privacy in their locations and movements over a period of time and that the police were therefore required to obtain a warrant to conduct GPS surveillance. *See Weaver*, 12 N.Y.3d at 441-42, 447. When *Weaver* was decided, it had long been established that individuals have reasonable expectations of privacy in movements and activities within their home. *See United States v. Karo*, 468 U.S. 705, 714-15 (1984) (holding that location tracking implicates Fourth Amendment privacy interests when it reveals information about individuals inside the home). In *Weaver*, the Court took a step further—one not previously taken by the United States Supreme Court—to recognize that even when the movements take place in public, “[t]he whole of a person’s progress through the world” will reveal “with breathtaking quality and quantity . . .

a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.” *Weaver*, 12 N.Y.3d at 441-42, 447. The Court found it “obvious” that such information is protected by “any reasonable notion of personal privacy or ordered liberty.” *Id.* at 441. At least five current justices of the Supreme Court recently reached the same conclusion in their concurrences in *United States v. Jones*, finding that long-term surveillance in investigations of most offenses would infringe on reasonable expectations of privacy. *Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring, joined by Ginsburg, J., Breyer, J., and Kagan, J.) (“[S]ociety’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.”); *id.* at 955 (Sotomayor, J., concurring).<sup>15</sup>

Although this case does not involve GPS surveillance, the principle underlying *Weaver* and the *Jones* concurring opinions—that government cannot engage in long-term surveillance of a person’s locations and movements without a warrant—applies to any technology, like IP address tracking, that “facilitates a new . . . perception of the world in which the situation of an object may be followed and exhaustively recorded over . . . a practically unlimited period.” *Weaver*, 12 N.Y.3d at 441. Indeed, Justice Alito in *Jones* explicitly acknowledged the reality that emerging technology other than GPS surveillance can be used to monitor a person’s locations and movements over time at varying levels of accuracy. *See, e.g., Jones*, 132 S. Ct. at 963 (Alito, J., concurring) (identifying the proliferation of mobile devices as “[p]erhaps most

---

<sup>15</sup> The majority in *Jones* invalidated the installation of the GPS device on the narrow basis that it involved a physical trespass without a warrant. The majority stated that “[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to” the reasonable-expectations-of-privacy analysis. *Jones*, 132 S. Ct. at 953.

significant” of the emerging location tracking technologies).<sup>16</sup> Even prior to *Jones*, federal courts had begun to recognize that location information kept by cell phone companies concerning their subscribers could be used to “enable the tracking of the vast majority of Americans,” and to hold that such information was protected by the Fourth Amendment. *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011) (*EDNY Garaufis Opinion*) (concluding that cell-phone users maintain a reasonable expectation of privacy in long-term cell phone location records); *see also, e.g., In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010) (*S.D. Tex. Smith Opinion*) (holding that government cannot access two months of historical cell phone location data without a warrant).

The lower court failed to recognize that a database of the IP addresses used by a person can, like GPS devices or a database of cell phone location information, reveal that person’s locations and movements over time. *See supra* at 5-6. Even though one IP address reveals only limited information about a person’s location at that moment in time,<sup>17</sup> the accumulation of IP addresses used by Harris to connect to Twitter over a 108-day period would provide the D.A. with a sophisticated tool for mapping his locations and movements over that long period of time. The length of time at issue here distinguishes this case from *People v. Hall*, 86 A.D.3d 450, 452 (1st Dep’t. 2011), in which the First Department did not find a privacy interest in three days of

---

<sup>16</sup> Although IP address location data is less precise than GPS tracking records, Justice Alito’s acknowledgment of the various location tracking technologies available makes clear that the particular technology at issue does not have to be equally precise to implicate privacy concerns. *See Jones*, 132 S. Ct. at 963.

<sup>17</sup> The federal appellate court decisions rejecting reasonable expectations of privacy in IP addresses are distinguishable because they involved law enforcement using a small and discrete number of IP addresses to determine a person’s subscriber information, and they did not implicate concerns about monitoring movement. *See, e.g., United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). These cases, as well as a federal district court opinion holding that Twitter users do not have a reasonable expectation of privacy in their IP addresses, *see In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F.Supp.2d 114,138 (E.D. Va. 2011), were not decided under *Weaver* and were decided prior to *Jones*. As discussed in more detail below, *see infra* at 34-36, to the extent necessary, this is an occasion in which it would be appropriate for New York courts to read the state Constitution more broadly than the federal Constitution.

cell phone location information. If tracking an individual's movements for sixty-five days (*Weaver*) or twenty-eight days (*Jones*) violates a reasonable expectation of privacy, *see Weaver*, 12 N.Y.3d 433; *Jones*, 132 S. Ct. at 946, 955 (Sotomayor, J., concurring); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring), then tracking an individual's movements over 108 days surely violates such an expectation as well. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

As the Court of Appeals stated in *Weaver*, "[t]echnological advances have produced many valuable tools for law enforcement and, as the years go by, the technology available to aid in the detection of criminal conduct will only become more and more sophisticated." *Weaver*, 12 N.Y.3d at 447. These new technological advances require "judicial oversight," because otherwise, their use "presents a significant and, to our minds, unacceptable risk of abuse." *Id.* The lower court failed to follow this clear guidance when it held that the D.A. could obtain information that would reveal Harris's locations and movements over time on a mere subpoena, instead of on a warrant based on probable cause.

**B. Harris's Reasonable Expectation Of Privacy Is Not Eliminated Simply Because His IP Addresses Are In The Possession Of Twitter.**

1. The Third-Party Doctrine Does Not Apply To Information Like IP Addresses That Reveals Locations And Movements.

The lower court held that Harris did not have an expectation of privacy in the requested information because that information is in the possession of a third party provider of Internet services, Twitter, not Harris. *See June 30 Order* at 4. The court reached that conclusion by relying on the so-called "third-party doctrine," which holds that individuals do not have a reasonable expectation of privacy in certain information voluntarily conveyed to third parties,

like bank and telephone records. *See People v Di Raffaele*, 55 N.Y2d 234 (1984) (telephone toll-billing records); *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank records); *Smith v. Maryland*, 442 U.S. 735, 742-45 (1979) (telephone dialing information. That reliance was erroneous, for three principal reasons.

First, the third-party doctrine does not apply here because, unlike bank records and telephone records, IP address information is not conveyed to a third party knowingly and voluntarily. The third-party doctrine developed on the premise that individuals lose their expectations of privacy when they “voluntarily” convey records to a third party. *See, e.g., Miller*, 425 U.S. at 440 (holding that bank records fall outside the protected zone of privacy because they relate to transactions to which the banks are parties); *Smith*, 442 U.S. at 742-44 (holding that telephone subscribers cannot harbor expectations of privacy in dialing information because they know that the phone company is receiving and storing that numerical information). By contrast, the doctrine does not apply where, as here, a person has not voluntarily or knowingly shared his location information with a third party “in any meaningful way.” *In re U.S. for an Order Directing a Provider of Elect. Commc’n Serv. to Disclose Records to the Government*, 620 F.3d 304, 317 (3d Cir. 2010). Thus, in the only federal appellate decision on the issue, the Third Circuit held that a cell phone user does not voluntarily share location information with a cell phone company in “any meaningful way,” because it is “unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information.” *Id.* Other federal courts have come to the same conclusion: conveyance of location information to a cell phone provider “is neither tangible nor visible to a cell phone user” and “is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal.” *S.D. Tex. Smith Opinion*, 747 F. Supp. 2d at 844; *In re U.S. for an*

*Order Authorizing Installation & Use of a Pen Register & a Caller ID Sys. on Tel. Nos.*, 402 F. Supp. 2d 597, 605 n.12 (D. Md. 2005) (rejecting analogy between cell phone location information and dialed telephone numbers because cell phone location information “is not affirmatively and actively conveyed by the phone’s possessor; the cell phone transmits the information automatically without the possessor’s awareness and possibly without his knowledge”).

Just like cell phone location information, IP address location information is communicated from an Internet user’s computer to automated equipment automatically, passively, invisibly, and unknowingly—most people do not even know what an IP address is—meaning that, as with cell phone location information, it is not voluntarily or knowingly conveyed by the user to Twitter (or other Internet services) in any meaningful way. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 586 (2011) (arguing that disclosure to automated Internet systems rather than to human beings should not fall under the third-party doctrine because it would otherwise eliminate protection for personal information transmitted over the Internet).

Second, an exception to the third-party doctrine exists where “society’s recognition of a particular privacy right as important swallows the discrete articulation of [the third-party doctrine].” *EDNY Garaufis Opinion*, 809 F. Supp. 2d at 124. The U.S. Supreme Court implicitly recognized this exception in *Smith* when, in applying the third-party doctrine, it contrasted the “limited” nature of the pen register/telephone dialing information that the government was seeking in that case with information conveyed to third parties in other circumstances where Fourth Amendment protections are not lost. *See Smith*, 442 U.S. at 741-42; *see also Doe v. Ashcroft*, 334 F. Supp. 2d at 510 (“The Court doubts that the result in *Smith*

would have been the same if a pen register operated as a key to the most intimate details and passions of a person's private life.”). For example, it is well-established that telephone conversations are protected even though people use third-party telephone companies to transmit the contents of their conversations, *Katz v. United States*, 389 U.S. 347, 352 (1967); letters are protected even though people must send them through the third-party postal service, *Ex parte Jackson*, 96 U.S. 727, 733 (1877); and emails are protected even though they are sent through third-party ISPs, *Warshak*, 631 F.3d at 285-86.

Because *Weaver* determined that it is “obvious” that society considers location and movement information to be highly private, *Weaver*, 12 N.Y.3d at 441-42, 447, and because IP addresses reveal such information, they fall under the same exception to the third-party doctrine as telephone conversations, letters, and e-mails. Although telephone conversations, letters, and e-mails are often referred to as “content” information, “there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private.” *EDNY Garaufis Opinion*, 809 F. Supp. 2d at 125. Because location records “implicate sufficiently serious protected privacy concerns . . . an exception to the third-party-disclosure doctrine should apply to them, as it does to content, to prohibit undue governmental intrusion.” *Id.* at 126; *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, No. 10 MC 0897, 2010 WL 5437209, at \*3 (E.D.N.Y. Dec. 23, 2010) (Orenstein, Mag. J.) (holding that the third-party doctrine should not apply to location records because “location information is not a simple business record and . . . it can effectively convey details that reveal the most sensitive information about a person’s life”). This Court should conclude the same as to IP addresses that similarly reveal location and movement information.

Finally, application of the third-party doctrine here would undermine the Court of Appeals' decision in *Weaver* to protect people's reasonable expectations of privacy in their locations and movements. As Justice Sotomayor recognized in her concurrence in *Jones*, the third-party doctrine is "ill suited to the digital age," in which third parties hold an increasing amount of people's private information. *Jones*, 132 S. Ct. at 957; *see also* Tokson, *supra*, at 588 ("Internet users generate enormous quantities of data, much of it stored by their online service providers," such as "[e]-mails, web-surfing histories, cloud computing documents, search terms, and credit-card information"); Stephen E. Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information From Unreasonable Search*, 55 Cath. U. L. Rev. 373, 412 (2006) (stating that the Fourth Amendment would provide little meaningful protection "[g]iven modern technology, if we retain no reasonable expectation of privacy in what we give to others"). That is especially true for movement information—our locations and movements are constantly tracked and stored silently by third parties, whether by cell phone companies or by websites. Rejecting the application of the third-party doctrine to such information is central to preserving the expectation of privacy in locations and movements recognized in *Weaver* and to ensuring that new technologies do not "erode the privacy guaranteed by the Fourth Amendment," *Kyllo v. United States*, 533 U.S. 27 at 34 (2001); *see also* *Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

2. The Third-Party Doctrine Should Not Be Controlling Under The New York Constitution.

Even if the third-party doctrine were to apply to the records at issue here under the Fourth Amendment, this Court should follow the lead of the Court of Appeals in *Weaver* and take this opportunity to hold that the third-party doctrine does not eviscerate people's reasonable



expectations of privacy in locations and movements over time under Article I, Section 12 of the New York Constitution. The New York Constitution has been interpreted to provide greater protections than the federal Constitution when circumstances warrant, such as in *Weaver*, when the Court of Appeals decided that prolonged GPS surveillance infringes on reasonable expectations of privacy. *See Weaver*, 12 N.Y.3d at 445; *People v. P.J. Video*, 68 N.Y.2d 296, 304-05 (1986) (citing numerous search-and-seizure cases in which New York courts have adopted standards independent from the federal Constitution).

The protections of the New York Constitution should be held to be broader than the federal Constitution where, as here, “doing so best promotes ‘predictability and precision in judicial review of search and seizure cases and the protection of the individual rights of our citizens.’” *Weaver*, 12 N.Y.3d at 445 (quoting *P.J. Video*, 68 N.Y.2d at 305). Such predictability and precision can be achieved when courts “provide and maintain ‘bright line’ rules to guide the decisions of law enforcement and judicial personnel who must implement [the court] decisions in their day-to-day operations in the field.” *P.J. Video*, 68 N.Y.2d at 305.

This case presents the appropriate occasion for the Court to announce a bright line rule that under the New York Constitution, law enforcement must obtain a warrant based on probable cause to obtain any set of data—including IP addresses—that reveals a person’s locations and movements over time, even when, as here, that data is possessed by third parties. As explained above, this bright-line rule is necessary to protect the privacy interest recognized by *Weaver* against emerging current and future technologies that allow people’s movements to be tracked. Eleven states have already rejected in some form the applicability of the federal third-party doctrine to their state constitutions, with the New Jersey Supreme Court holding that individuals maintain a reasonable expectation of privacy in subscriber information, including IP addresses,

provided to an ISP under the New Jersey Constitution. See *New Jersey v. Reid*, 194 N.J. 386, 399-400 (2008); Henderson, *supra*, at 395 (surveying states that reject the third-party doctrine). This Court should, at a minimum, hold that individuals maintain a reasonable expectation of privacy in information that they convey to a third party where, as here, the information implicates a privacy interest that has been accepted as important by the New York Court of Appeals.

As the Court explained in *Weaver*:

The alternative would be to countenance an enormous unsupervised intrusion by the police agencies of government upon personal privacy and, in this modern age where criminal investigation will increasingly be conducted by sophisticated technological means, the consequent marginalization of the State Constitution and judiciary in matters crucial to safeguarding the privacy of our citizens.

*Weaver*, 12 N.Y.3d at 445.

### CONCLUSION

For the foregoing reasons, *Amici* respectfully request that the Court reverse and vacate the lower court's decisions and hold that Twitter users like Harris have standing to challenge government demands to third parties for information that implicates their constitutional rights and that the Twitter Subpoena violates Harris's First and Fourth Amendment rights.

Dated: August 27, 2012

Respectfully submitted,



Aden J. Fine  
American Civil Liberties Union Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
Telephone: (212) 549-2693  
Attorney for Amicus Curiae AMERICAN CIVIL  
LIBERTIES UNION FOUNDATION

Mariko Hirose  
Arthur Eisenberg  
New York Civil Liberties  
Union Foundation  
125 Broad Street, 19th Floor  
New York, New York 10004  
Telephone: (212) 607-3300  
Attorneys for Amicus Curiae NEW YORK CIVIL  
LIBERTIES UNION FOUNDATION

Marcia Hofmann  
Hanni Fakhoury  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: (415) 436-9333 x. 116  
Attorneys for Amicus Curiae ELECTRONIC  
FRONTIER FOUNDATION

Paul Alan Levy  
Public Citizen Litigation Group  
1600 20th Street, NW  
Washington, D.C. 20009  
Telephone: (202) 588-1000  
Attorney for Amicus Curiae PUBLIC CITIZEN,  
INC.

# EXHIBIT A

**SUBPOENA (DUCES TECUM)****FOR A WITNESS TO ATTEND THE  
CRIMINAL COURT OF THE CITY OF NEW YORK**

In the Name of the People of the State of New York

To: Twitter, Inc.  
c/o Trust & Safety  
795 Folsom Street  
Suite 600  
San Francisco, CA 94107

**YOU ARE COMMANDED** to appear before the **CRIMINAL COURT** of the County of New York, **PART JURY 7**, at the Criminal Court Building, 346 Broadway, between Hogan Place and White Street, in the Borough of Manhattan, of the City of New York, on February 8, 2012 at 9:00 AM, as a witness in a criminal action prosecuted by the People of the State of New York against:

**MALCOLM HARRIS**

and to bring with you and produce the following items:


Any and all user information, including email address, as well as any and all tweets posted for the period of 9/15/2011-12/31/2011 for the following twitter account:

**@destructuremal**  
<http://twitter.com/destructuremal>

**IF YOU FAIL TO ATTEND AND PRODUCE SAID ITEMS**, you may be adjudged guilty of a Criminal Contempt of Court, and liable to a fine of one thousand dollars and imprisonment for one year.

Dated in the County of New York,  
January 26, 2012

CYRUS R. VANCE, JR.  
District Attorney, New York County

By:   
Lee Langston  
Assistant District Attorney  
212 335-9206

Case #: 2011NY080152

**TWITTER IS DIRECTED** not to disclose the existence of this subpoena to any party. Such disclosure would impede the investigation being conducted and interfere with the enforcement of law.