CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK: JURY 7

The People of the State of New York, -Against- Malcolm Harris, Defendant.	Docket No.: 2011NY080152

MEMORANDUM OF AMICI CURIAE IN SUPPORT OF NON-PARTY TWITTER, INC.'S MOTION TO QUASH § 2703(d) ORDER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

INTRODUCTION

This Court's April 20, 2012 Order requires Twitter to provide the New York County District Attorney's Office with a broad swath of information about a Twitter user's communications, locations, and movements over a three-and-a-half month period. That information includes the content of the user's "tweets," the date, time, and Internet Protocol address that corresponds to each time the user, Malcolm Harris, logged in to his Twitter account, and the amount of time each log-in lasted, regardless of whether he posted any tweets during those times or whether any of his tweets are related to the D.A.'s pending disorderly conduct prosecution of Harris. The Order, which permits the D.A. to obtain all of this information without obtaining a warrant, violates Harris's First and Fourth Amendment rights, as well as his corresponding rights under the New York Constitution.

Equally troubling, the Court's Order held that Harris—and by implication, the thousands of other Twitter users residing in New York—does not have standing to challenge the D.A.'s broadly worded trial subpoena that did not comply with the statute purportedly authorizing it, let alone the Constitution. That holding is at odds with numerous decisions from the United States Supreme Court and courts around the country that make clear that individuals whose constitutional 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.

Amici Curiae the American Civil Liberties Union, the New York Civil Liberties Union, the Electronic Frontier Foundation, and Public Citizen (collectively, "*Amici*") therefore 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 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 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. Commc'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 225,000 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 BACKGROUND

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 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 e-mail 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—*i.e.*, Harris's account.[1] 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 his tweets, the date, time, and the Internet Protocol ("IP") address[2] 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 Subpoena—"[a]ny and all user information"—also appear to encompass information concerning

[1] A copy of the Twitter Subpoena is attached hereto as Exhibit A.
[2] An IP address is a unique numerical address that identifies individual computers or other devices as they interact over the Internet. IP addresses can be used to determine where a computer and its user are located when it is connected to the Internet.

Harris's use of Twitter's "Direct Message" feature, which is the functional equivalent of a private email message service between Twitter users and their friends. Some of the information, like IP addresses and information concerning Direct Messages, was never publicly available; other information, like the content of the tweets, was once (but is no longer) publicly available via Twitter.

The D.A. did not notify Harris of the issuance of the Twitter Subpoena. In fact, without any authority, the D.A. "direct[ed]" Twitter not to inform Harris of the existence of the trial subpoena. *See* Ex. A. Harris learned of the subpoena only because Twitter notified him of it, pursuant to Twitter's policy of informing its customers of such subpoenas unless it is legally restricted from doing so.

Harris filed a motion to quash the Twitter Subpoena on February 6, 2012. The D.A. filed a brief in opposition, and took the position that Harris did not have standing to challenge the Twitter Subpoena. In its brief, the D.A. alleged 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.

On April 20, 2012, the Court denied Harris's motion, holding that he had no standing to challenge the Twitter Subpoena. The Court also proceeded to consider the validity of the Subpoena, concluding that it complied with the Stored Communications Act (the "SCA"), 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.

Harris filed a motion to reargue on April 30, 2012, to which the D.A. filed a response. 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 Court.

ARGUMENT

I. TWITTER USERS HAVE STANDING TO MOVE TO QUASH SUBPOENAS THAT IMPLICATE THEIR CONSTITUTIONAL RIGHTS.

The Court's April 20 Order held that Harris does not have standing to challenge the Twitter Subpoena on the ground that it was issued to Twitter, not to Harris, for information in Twitter's possession, not in Harris's possession, and that Harris's constitutional rights are therefore not threatened by the subpoena. Order at 4-6. That conclusion is at odds with decisions from the United States Supreme Court and numerous courts around the country. Because Harris's First Amendment rights are implicated by the Twitter Subpoena, he has standing to challenge it.

A. Twitter Users Have Standing To Challenge Third-Party Disclosure Requests.

"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). Because Harris's First Amendment rights are implicated by the Twitter Subpoena, he has standing to challenge its validity, even if

he disclosed some of the requested information to Twitter and even if the Court ultimately determines that his rights were not violated.[3]

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. 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 cannot 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").

Eastland is consistent with other Supreme Court cases. *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 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

[3] 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. United States*, 439 U.S. 128, 139-40 (1979); *People v. Laws*, 623 N.Y.S.2d 216, 218 [1st Dept. 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 22-29.

rights)[4]; *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).

Courts around the country, including courts in New York, have followed the Supreme Court's clear guidance and held 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.[5]

In reaching its prior conclusion, this Court relied heavily on Twitter's Terms of Service and its Privacy Policy. Those terms of service and the privacy policy, like the similar ones of many other Internet companies, do not alter the First Amendment standing analysis. Indeed, in *In re Grand Jury Subpoena No. 11116275*, Misc. No. 11-527 (RCC), 2012 WL 691599 (D.D.C. Feb. 23, 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

[4] A *per curiam* affirmance 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*).

[5] *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 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).

seeking 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).[6]

That Harris has already disclosed some of the subpoenaed information to Twitter similarly does not eliminate his 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 did not have "a possessory interest in the documents 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 reversed on other grounds*, *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (same). Were it otherwise, Internet users would never be able to defend their constitutional right to engage in anonymous speech on the Internet, because users must provide their information to others—e.g., to Internet Service Providers—to access the Internet. As Judge Marrero, a federal district court judge in the Southern District of New York, explained in a similar situation:

> [T]he implications of the Government's position 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.

[6] As Twitter's motion makes clear, 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. Twitter Memorandum at 4.

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 anonymous speech 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, New York County 2005] (adjudicating motion to quash subpoena by anonymous Internet user whose identifying information was being sought from ISP); *Greenbaum v. Google, Inc.*, 845 N.Y.S.2d 695, 698 [Sup Ct, New York County 2007] (same); *Cohen v. Google, Inc.*, 887 N.Y.S.2d 424 [Sup Ct, New York County 2009] (same); *Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010) (same).[7]

The bank records cases previously relied on by the D.A. and the Court are not to the contrary. 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. *Id*. at 444 n.6; *see also In re First Nat'l Bank*, 701 F.2d at 117-18 (rejecting the government's assertion that the Supreme Court's decision in *Miller* forecloses petitioners from having standing to challenge a third-party request). "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; *see also Local 1814*, 667 F.2d at 271 (same).

[7] *See also Anonymous Online Speakers v. United States District Court*, 661 F.3d 1168 (9th Cir. 2011); *Doe v. Cahill*, 884 A.2d 451, 457 (Del. 2005); *Dendrite Int'l, Inc. v. Doe*, 775 A.2d 756 (N.J. App. 2001); *Mobilisa, Inc. v. Doe 1*, 170 P.3d 712 (Ariz. App. 1B 2007); *Indep. Newspapers, Inc. v. Brodie*, 966 A.2d 432 (Md. 2009); *Pilchesky v. Gatelli*, 12 A.3d 430 (Pa. Super. 2011); *Krinsky v. Doe 6*, 72 Cal. Rptr. 3d 231 (App. 6th 2008); *In re Does 1-10*, 242 S.W.3d 805 (Tex. App. 2007); *Solers, Inc. v. Doe*, 977 A.2d 941 (D.C. 2009).

One of the principal rationales behind *Eastland* and all of these other cases is that even if subpoenas are directed to third parties, individuals whose rights are at stake must still be given an opportunity to challenge them because 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, New York 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.").

Although Twitter has now filed its own motion in this case, that does not mean that it will do so in other cases. Indeed, its brief makes clear that one of the reasons why Twitter weighed in here is because of the potential consequences for Twitter of the 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. Twitter Memorandum at 5. The reality is that Twitter, like other Internet 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)).[8]

[8] It is well-established that 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), *reversed on other grounds*, *RIAA v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003) (holding that Verizon had standing to

Because Twitter and similar entities do not have the incentives to challenge these government requests—in large part because their own rights are not primarily at stake—Internet users, the individuals whose constitutional rights are at stake, are precisely the people who should have standing to try 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.").[9] The same holds here: 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.[10] Given the First Amendment interests at stake here, *see* Part I.B, in addition to the Fourth Amendment interests, *see* Part II.B, Harris has standing to challenge the Twitter Subpoena.

B. Harris Has Standing Because His First Amendment Rights Are Implicated By The Twitter Subpoena.

Government demands for information concerning an individual's expressive activities 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

---

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).

[9] In order for the individual whose rights are at stake to assert her rights in court, she must have notice of the existence of the subpoena. The Stored Communications Act facilitates this by specifically requiring that the government give prior notice to a user or a subscriber when issuing subpoenas for certain information, including information sought by the Twitter Subpoena. 18 U.S.C. § 2703. The D.A. did not provide the prior notice here, and contrary to the Court's conclusion, the D.A. cannot rely on Twitter to give prior notice to the user of the existence of a subpoena.

[10] 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.

the investigative process tends to impinge upon such highly sensitive areas as freedom of speech or press, freedom of political association, 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). Because the Twitter Subpoena would reveal sensitive details about Harris and his communications, he has standing to raise a First Amendment challenge to it.

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. This type of prolonged, wholesale surveillance into speech activities implicates the First Amendment. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.") (internal quotation marks omitted); *People v. Collier*, 85 Misc. 2d 529, 554 [Sup Ct, New York County 1975] ("Our society, with its rich tradition of law and limited government, is deeply dedicated to privacy, individual freedom and political tolerance. 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 can monitor their speech and that they may be held accountable for what they say, people will be less inclined to speak as freely. That is especially the case with respect to "casual," spontaneous speech, because individuals would likely refrain from publicly making such statements as often if they thought that the government might later obtain those statements and hold the statements

against them—a particularly harmful result for Internet speech, especially for speech occurring on websites like Twitter.[11]

The government surveillance at issue here is especially concerning because, in addition to the content of Harris's tweets, the Twitter Subpoena also covers the IP addresses associated with Harris's use of Twitter, and the date and time for each log-in session. IP addresses correlate to specific geographic locations. *See, e.g.*, *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409 (2d Cir. 2004) (explaining that the IP address identifies the location of the device being used); *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"). The aggregation of this information will, thus, provide the D.A. with a comprehensive and detailed map of where Harris was when he was expressing certain thoughts or simply reading others' tweets, over a three-and-a-half month period, regardless of whether there is any connection between those tweets and the pending prosecution.

The combination of Harris's location plus the content of his messages makes the Twitter Subpoena particularly invasive from a First Amendment perspective, because knowing Harris's location when he was expressing certain thoughts will provide meaning to some of his tweets. For example, a message like "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"

[11] That the content of Harris's tweets was public at some point does not undermine Harris's First Amendment interest in precluding the government from needlessly inquiring into his speech activities. Courts have recognized that forced disclosure of content that was once publicly available may still chill speech. *See Comty.-Serv. Broad. of Mid-Am., Inc. v. FCC*, 593 F.2d 1102, 1122 (D.C. Cir. 1978) (holding that a requirement that government-funded non-commercial radio stations tape-record all public affairs programs and make the recordings available to FCC Commissioners was invalid because it was likely to chill free expression and no legitimate government interest was truly being served).

might mean one thing if tweeted from Woodstock on the night of a Bob Dylan concert, but something far different if tweeted from Tehran 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, 2011. 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. Connecting Harris's specific locations to his specific messages will, thus, provide the D.A. with nuanced insight into Harris's daily life and his expressive activities.

Knowing how long Harris was logged on to Twitter when he tweeted certain thoughts, or when he was simply reading others' tweets—items also encompassed by the Twitter Subpoena—will similarly provide details about Harris's reading and speaking habits. In addition, the IP addresses will disclose exactly how Harris accessed Twitter to communicate—e.g., through a laptop, his mobile phone, or his home computer—providing yet more personal details about Harris's communications.

On their own, some of these details about Harris's communications might not be terribly invasive. Combined over such a long period of time, however, these discrete details and data points will 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").[12] Where individuals are when they say a certain thing or read certain material, when they say those things or read other things, how long they spend to say those things or to read other things, and what kind of tools they use for their communications, are private, intimate details about individuals' communications and communications habits. None of this information is the government's business, and the D.A. cannot simply obtain it without first satisfying constitutional scrutiny. *See, e.g.*, *Lamont v. Postmaster General*, 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*, 85 Misc. 2d at 556 (explaining that even small infringements of constitutional rights cannot be permitted).

Moreover, although the D.A. has now disclaimed any intent to seek information concerning Harris's use of Twitter's "Direct Messaging" feature, which essentially functions like a private email account, 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 never to 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 are intended to be private and are viewable only by the individuals

[12] 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.

communicating with each other via direct messages. The content of those direct messages is indisputably constitutionally protected, much like the content of emails and telephone calls. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2011) (holding that the content of emails cannot be obtained by the government unless constitutional scrutiny is first satisfied); *Katz v. United States*, 389 U.S. 347, 352-53 (1967) (same re telephone calls). In addition to revealing the content of those private communications, information concerning Harris's Direct Messages would also disclose 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.

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. 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 the right to personal privacy and free speech. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). The ease in which

information is spread over the Internet—especially through Twitter and similar services—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 like 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, countless individuals likely *will be* chilled by the government's demand for information about individuals' Internet communications.[13]

Because Harris's First Amendment rights are, thus, implicated by the Twitter Subpoena, he has standing to challenge it.

[13] The Court should be careful not to permit even a seemingly small encroachment on constitutional rights. *See, e.g., Boyd v. United States*, 116 U.S. 616, 635 (1886), *overruled on other grounds by Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294 (1967) ("It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedures. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed."); *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.").

II. THE TWITTER SUBPOENA AND THE RESULTING COURT ORDER VIOLATE HARRIS'S CONSTITUTIONAL RIGHTS.

Turning to the merits, the Twitter Subpoena and the Court's April 20 Order violate Harris's First and Fourth Amendment rights, as well as his corresponding rights under the New York Constitution.

A. The Twitter Subpoena and the Court's § 2703(d) Order Violate The First Amendment And Article I, Section 8 Of The New York Constitution.

Because the Twitter Subpoena and the Court's § 2703(d) order 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. *See, e.g.*, *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*, 85 Misc. 2d at 560 ("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 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 published the tweets on that account in the past. 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 information from Twitter, let alone 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. Detailed information concerning his use of Twitter and his locations and movements on the other 107 days covered by the Twitter Subpoena is not necessary for that purpose.

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, all the D.A. needs are those specific tweets. Again, the D.A. does not need any information about Harris's locations and movements or his Twitter activities for any of the other hundred-plus days to establish any such contradictions. Nor is there any reason why the D.A. would need the content of his tweets from the day in question that had nothing to do with the Brooklyn Bridge incident, to the extent there were such tweets. In its opposition to Harris's motion to re-argue, the D.A. reiterates that "the information requested by the People is directly germane to the contested issue of defendant's state of mind at the time he chose to defy police orders and block

the Brooklyn Bridge." Affirmation In Support Of People's Response To Defendant's Motion To Reargue at 7. Regardless of whether that is so, Harris's "state of mind" on all of the other days—let alone his specific whereabouts, at various times of each day, and how long he spent using Twitter—is unrelated to his state of mind on the day in question. 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; *Collier*, 85 Misc. 2d at 560; *United States v. Bursey*, 466 F.2d 1059, 1083 (9th Cir. 1972); *Amazon.com v. Lay*, 758 F. Supp. 2d at 1169 & n.2 (invalidating disclosure demand because the information requested was not necessary to accomplish North Carolina's stated goals).[14]

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 (considering the validity of a third-party subpoena and holding that, "(E)ven though the governmental purpose (assuring teacher competence) be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved") (quoting *Shelton v. Tucker*, 364 U.S. 479, 488 (1960) (quotation marks omitted)).

[14] 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 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.

The Twitter Subpoena fails to "use a scalpel" because it broadly seeks "[a]ny and all user information" over a long period of time, even though the D.A. cannot claim that all—or even most—of Harris's tweets have anything to do with the Brooklyn Bridge incident or Harris's state of mind at the time of the incident. For example, if Harris posted a Tweet two weeks before the incident about a new book he read or about the New York Yankees, or even if he did so on the day in question, there is no need for the government to obtain that tweet. Nor does the D.A. need information about where Harris was at that time and for how long he was logged on to Twitter. Indeed, the D.A. has not articulated 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 acknowledges 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*, 829 F.2d 1291, 1302 (4th Cir. 1987) (quashing a subpoena requiring videotape distributers 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 whether an item is to be produced or not"); *Amazon.com v. Lay*, 758 F. Supp. 2d at 1169 (holding that the government's demand 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 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. 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 the review can implicate Harris's First Amendment interests. *See N.Y. Times Co. v. Jascalevich*, 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); *Bradosky 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). In any event, even if an *in camera* review were deemed appropriate, the Court should release information to the D.A. only if the D.A.'s request can pass constitutional muster, not just if the Court deems the information to be relevant to the case.

B. The Twitter Subpoena And The Court's § 2703(d) Order Violate 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 to be free of government surveillance of his movements over a period of time. Although some of the information requested here was publicly available at one point, a significant portion, such as the IP addresses and information concerning Direct Messages, never was publicly available. In addition, some of the formerly public tweets are no longer publicly available via Twitter. The government cannot obtain this information—Twitter's database of historical speech activities and its users' corresponding locations and movements—without a warrant based on probable cause; a mere subpoena or a § 2703(d) order is not sufficient.[15]

[15] Independently of the Fourth Amendment, the SCA protects the contents of the tweets even if they may once have been publicly available via Twitter. As Twitter's memorandum in support of its motion to quash explains, *see* Memorandum at 7, under the express terms of the Stored Communications Act, the D.A. cannot obtain the contents of many of Harris's tweets from Twitter without first obtaining a search warrant. 18 U.S.C. § 2703(a); *see also id.* at 18 U.S.C. § 2703(b)(1)(B)(ii). The cases cited by the D.A. in an earlier brief for the proposition that publicly available information is not covered by the SCA are not to the contrary, as those cases involve information that is currently "readily accessible to the general public." 18 U.S.C. § 2511(2)(g). At most, the cases support only the self-evident point that the SCA provides no liability for viewing publicly accessible communications.

The New York Court of Appeals has recognized that individuals have a reasonable expectation of privacy in their movements over a prolonged period of time, even movements conducted in public places, and that a warrant is required for the government to obtain that information because it can reveal intimate details about people's lives. *See People v. Weaver*, 12 N.Y.3d 433, 441-42 [2009]. As the Court of Appeals explained in *Weaver*: "Cell technology has moved presumptively private phone conversation from the enclosure of *Katz*'s phone booth to the open sidewalk and the car, and the advent of portable computing devices has resituated transactions of all kinds to relatively public spaces. It is fair to say, and we think consistent with prevalent social views, that this change in venue has not been accompanied by any dramatic diminution in the socially reasonable expectation that our communications and transactions will remain to a large extent private." *Id*. at 442-43.

At least five current justices of the United States Supreme Court have come to the same conclusion. In *United States v. Jones*, 132 S. Ct. 945 (2012), Justice Alito, writing for himself and three other concurring members, and Justice Sotomayor, in her separate concurrence, opined that the use of GPS monitoring over a period of twenty-eight days—*i.e.*, long-term location tracking—impinges on an individual's reasonable expectation of privacy. *Id*. at 964 (Alito, J., concurring); *see also id.* at 955 (Sotomayor, J., concurring). As Justice Alito explained: "[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 964.

This case does not involve GPS surveillance, as in *Weaver* or *Jones*. But the accumulation of IP addresses over a 108-day period likewise provides law enforcement with a sophisticated tool for mapping an individual's specific whereabouts over time, thus burdening

the individual's constitutionally protected right to move freely without government surveillance. *Cf. City of Chicago v. Morales*, 527 U.S. 41, 54 (1999) ("[I]t is apparent that an individual's decision to remain in a public place of his choice is as much a part of his liberty as the freedom of movement inside frontiers that is 'a part of our heritage'); *Papachristou v. City of Jacksonville*, 405 U.S. 156, 164 (1972) (stating that activities like wandering and strolling from place to place are "historically part of the amenities of life as we have known them"). That is because IP addresses, like GPS devices, can reveal one's geographic locations and movements from one place to another. *See, e.g.*, *Register.com*, 356 F.3d at 409; *Sony Music*, 326 F. Supp. 2d at 567. Thus, by using the IP addresses linked to each date and time that Harris logged into Twitter over a three-and-a-half month period, the government can determine his location at the very times that he was engaged in publishing his own messages or reading others' thoughts—regardless of whether the underlying speech was related to the subject matter of this prosecution, and regardless of whether he was using Twitter from a public or a private space, including Harris's home, where his expectation of privacy is greatest.[16]

That the D.A. sought three-and-a-half months of data distinguishes this case from *People v. Hall*, 86 A.D.3d 450, 452 [1st Dept 2011], in which the First Department did not find a privacy interest in three days of cell phone-based location information. Indeed, if tracking an individual's movements in a vehicle for twenty-eight days (*Jones*) or for sixty-five days (*Weaver*) violates a reasonable expectation of privacy, *see Jones*, 132 S. Ct. at 946; *Weaver*, 12 N.Y.3d 433, then tracking an individual's movements over 108 days surely violates such an

[16] 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 one of several tools that allow Internet users to obfuscate their IP addresses. Although IP address location data is less precise than GPS tracking records, it does not have to be equally precise to implicate privacy concerns. Indeed, Justice Alito's opinion makes clear that his conclusion did not depend on the particular type of tracking technology at issue in *Jones*, and that he was well aware that the government can also track location through numerous other means, existing and not yet imagined. *Jones*, 132 S. Ct. at 963 (identifying the proliferation of mobile devices as "[p]erhaps most significant" of the emerging location tracking technologies).

expectation as well. *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.").

That is especially the case given that Twitter users like Harris increasingly rely on laptops, iPads, or other mobile devices to access Twitter. They are likely to carry their devices with them at all times and to be logged on to Twitter for a significant portion of the day, enabling the government to reconstruct their movements to conduct virtually twenty-four hour surveillance of them as they traverse both public and private spaces, much like in *Jones* and *Weaver*.[17]

Technological advances have made possible government fishing expeditions into databases of information and communications that would have been impossible in the past. Although the government always could have attended a suspect's public speeches in the course of its investigations, it has never before had the capacity to review, in retrospect, the content and location of every public speech made by a criminal defendant for a three-plus month period. In this way, Twitter's database "is not a mere enhancement of human sensory capacity, it facilitates a new technological perception of the world." *Weaver*, 12 N.Y.3d at 441; *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive."). As the Court of Appeals stated in *Weaver*, in words that could have been written for this case: "Technological advances have produced many valuable tools for law enforcement

[17] Indeed, IP addresses can be cross-referenced with records from other companies to provide information reflecting an individual's activities at home, "the very core" of the Fourth Amendment's right to be free from unreasonable government searches. *Silverman v. United States*, 365 U.S. 505, 511 (1961). For example, the information the D.A. seeks here may reveal that Harris frequently logged into Twitter from a specific IP address. An information demand to the company that assigned that IP address—not an unlikely scenario given that the D.A. expressly demanded Harris's personal email address— may reveal that the number corresponds to a computer or network in Mr. Harris's home.

and, as the years go by, the technology available to aid in the detection of criminal conduct will only become more and more sophisticated. Without judicial oversight, the use of these powerful devices presents a significant and, to our minds, unacceptable risk of abuse." 12 N.Y.3d at 447.

That the Court has now approved the validity of the Twitter Subpoena and issued its own § 2703(d) order does not cure these constitutional deficiencies. The Court has still not determined that there is probable cause to permit the D.A. to obtain all of this intimate and detailed information about Harris's communications, locations, and movements over such a lengthy period of time; in issuing the § 2703(d) order, the Court merely concluded that the D.A. had established that the information requested was "relevant and material" to a criminal investigation.

Nor does the fact that the information requested is in the possession of a third party mean that there can be no constitutional violations here. Prolonged location tracking violates citizens' reasonable expectations of privacy; that is true even where, as here, the information is stored by a third party. *See, e.g.*, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317-18 (3d Cir. 2010) (*Third Circuit Opinion*) (distinguishing cell phone location information maintained by the cell phone company from bank records or phone dialing information); *In re U.S. for an Order Authorizing the Release of Historical Cell-Site*, 809 F.Supp.2d 113, 126 (E.D.N.Y. 2011) ("[T]he court concludes that an exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records, despite the fact that those records are collected and stored by a third party."). Unlike the bank records and telephone records cases cited by the Court,[18] Internet users do not voluntarily share their

[18] *United States v. Miller*, 425 U.S. 435 (1976) (holding that an individual has no Fourth Amendment interest in bank records created and maintained by the bank in the course of financial transactions); *Smith v. Maryland*, 442

location information with their ISPs or the other Internet services they utilize in a manner that is analogous to the dialing of a telephone or engaging in a financial transaction with a bank. In addition, whereas banking records and telephone dialing information are knowingly and voluntarily provided to a third party, IP address information is communicated by the Internet user automatically, passively, invisibly, and unknowingly. *See Third Circuit Opinion*, 620 F.3d at 317 (rejecting an identical argument in the context of a demand for cell phone location information, and noting that it is "unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information," such that a "cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way"); *In re U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D.Tex. 2010) (holding that cell phone location data is different from the bank records discussed in *Miller* or the phone numbers dialed in *Smith*, because it "is neither tangible nor visible to a cell phone user" and because it "is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal"). Indeed, the vast majority of users have no idea what an IP address is or that it can be used to track their movements and locations.[19]

The information sought here by the Twitter Subpoena is also significantly different in character from bank or telephone records. It is rich in detail about an individual's communications and movements over time. For that reason, it is protected by the Constitution even where it is stored by, or sent and received through, third parties, *see Warshak*, 631 F.3d at 283-88, and even where it is otherwise observable by the public, *see Weaver*, 12 N.Y.3d at 441-

---

U.S. 735 (1979) (finding that the installation of a pen register to collect telephone numbers does not violate the Fourth Amendment rights of telephone customers); *People v Di Raffaele*, 55 N.Y2d 234 [Ct App 1984] (concluding that there is no privacy interest in telephone records that were voluntarily given to one's telephone company).

[19] Because of these differences, *amici* disagree with the conclusion of those courts that have applied the reasoning of the bank and telephone dialing records cases to IP address information. *See 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); *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, Misc. No. 1:11-DM-3, 2011 WL 5508991, at *18-19 (E.D. Va. Nov. 10, 2011).

42. Because "internet records of the type obtained via a [government demand] could differ substantially from transactional bank or phone records," *Doe v. Ashcroft*, 334 F. Supp. 2d at 509, this case presents a far different scenario from the bank and telephone dialing record cases. *Id*. at 510 ("In stark contrast to this potential to compile elaborate dossiers on internet users, the information obtainable by a pen register is far more limited . . . 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.").

Moreover, unlike the bank or telephone records cases, the government's subpoena seeks information implicating free speech rights, *see supra* Part I.B., creating First Amendment concerns not present in cases dealing only with locational privacy. Where, as here, First Amendment interests are implicated by a government search, Fourth Amendment scrutiny is heightened. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding that a search warrant implicating expressive rights must meet the warrant requirement with "scrupulous exactitude"); *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (same).

Even if the bank and telephone records cases are deemed controlling for Fourth Amendment purposes, that does not mean that Harris's separate and distinct rights under Article I, Section 12 of the New York Constitution are not violated by the Twitter Subpoena and the § 2703(d) order. *Weaver* is prescient on this point:

> We note that we have on many occasions interpreted our own Constitution to provide greater protections when circumstances warrant and have developed an independent body of state law in the area of search and seizure. We have adopted separate standards "when 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.'" What we articulate today may or may not ultimately be a separate standard. If it is, we believe the disparity would be justified. 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.

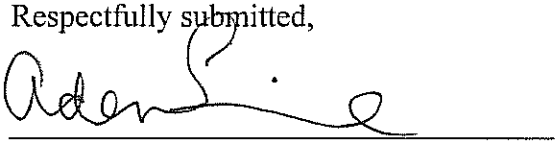
Weaver, 12 N.Y.3d at 445. This Court should follow the lead—and the instructions—of *Weaver*, and hold that, to the extent federal law and the protections of the Fourth Amendment do not cover the detailed, intimate Internet information at issue here, greater protection should be provided under the New York Constitution.

CONCLUSION

For the foregoing reasons, *amici* respectfully request that the Court grant the motion to quash and hold that Twitter users like Harris have standing to challenge government demands to third parties for information that implicates their constitutional rights, invalidate the subpoena, and vacate the § 2703(d) order.

Dated: May 31, 2012

Respectfully submitted,



Aden J. Fine
125 Broad St., 18th Floor
New York, NY 10004
Telephone: (212) 549-2693
Attorney for Amicus Curiae American Civil Liberties Union

Marcia Hofmann
Hanni Fakhoury
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.