

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

-----X

THE PEOPLE OF THE STATE OF NEW YORK

-AGAINST-

DECISION AND ORDER

Docket No.: 2011NY080152

MALCOLM HARRIS,

DEFENDANT.

-----X

MATTHEW A. SCIARRINO, JR., J.:

The New York County District Attorney's Office seeks to obtain the #Twitter records of @destructuremal using a #¹ subpoena. The defendant is alleged to have participated in a #OWS protest march on October 1, 2011. The defendant, Malcolm Harris, along with several hundred other protesters, were charged with Disorderly Conduct (P.L. §240.20[5]) after allegedly marching on to the roadway of the Brooklyn Bridge. The defendant moved to #quash that subpoena. That motion is #denied.

On January 26, 2012, the People sent a subpoena *duces tecum* to the online social networking service and microblogging service, Twitter, Inc. ("Twitter"). The subpoena seeks user information including email address, and Tweets posted for the period of September 15, 2011 to December 31, 2011, for the Twitter account @destructuremal, the Twitter account which is allegedly used by Malcolm Harris.

¹ The # symbol, called a hashtag, is used to mark keywords or topics in a Tweet. For example, if you search #OWS on Twitter you'll get a list of tweets that mention #OWS.

On January 30, 2012, after conferring with the District Attorney's office, Twitter informed the defendant that the Twitter account, @destructuremal, had been subpoenaed.² On January 31, 2012, the defendant notified Twitter of his intention to file a motion to quash the subpoena. Twitter then took the position that it would not comply with the subpoena until this court rules on the motion.

The defendant moves to quash the subpoena in his own right or to intervene in the proceedings to quash the subpoena. The People oppose the motion to quash and the motion to intervene.

DISCUSSION

² Twitter's Guidelines for Law Enforcement addresses any requests for users' information. Twitter's policy is that prior to disclosure, Twitter will notify its users when information is requested unless forbidden from doing so by statute or court order. (*See* <http://support.twitter.com/articles/41949-guidelines-for-law-enforcement>).

Twitter is an online social networking service that is unique because it enables its users to post (“Tweet”), repost (“Retweet”), and read the Tweets of other users. Tweets can include photos, videos, and text-based posts of up to 140 characters.³ Users can monitor, or “follow” other users’ Tweets, and can permit or forbid access to their own Tweets. Besides posting Tweets or reposting other users’ Tweets, users may also use the more private method to send messages to a single user (“Direct Message”). Each user has a unique username. In order to sign up to be able to use Twitter’s services, you must click on a button below a text box that displays Twitter’s Terms of Service (“Terms”). (See <https://twitter.com/signup>).

By clicking on a button on the registration web page, you are agreeing to all of Twitter’s Terms, including the Privacy Policy (see <https://twitter.com/privacy>). The Privacy Policy informs users about the information that Twitter collects upon registration of an account and also whenever a user uses Twitter’s services. Twitter collects many types of user information, including IP address, physical location, browser type, mobile carrier among other types. By design, Twitter has an open method of communication. It allows its users to quickly broadcast up-to-the-second information around the world. The Tweets can even become public information searchable by the use of many search engines. Twitter’s Privacy Policy informs the users that, “[w]hat you say on Twitter may be viewed all around the world instantly.” (See <https://twitter.com/privacy>). With over 140 million active users and the posting of approximately 340 million Tweets a day (see <http://blog.twitter.com/>), it is evident that Twitter has become a significant method of communication for millions of people across the world.

1. DEFENDANT’S STANDING TO MOVE TO QUASH THE PEOPLE’S SUBPOENA

The first issue that must be addressed is whether the defendant has standing to quash the subpoena served upon Twitter.

³ The reality of today’s world is that social media, whether it be Twitter, Facebook, Pinterest, Google+ or any other site, is the way people communicate and to some extent has supplemented email for many people. Twitter has also become the way many receive their news information. Twitter describes itself as, “[t]he fastest, simplest way to stay close to everything you care about.” (See <https://twitter.com/about>).

New York courts have yet to specifically address whether a criminal defendant has standing to quash a subpoena issued to a third-party online social networking service seeking to obtain the defendant's user information and postings.⁴ Nonetheless, an analogy may be drawn to the bank record cases where courts have consistently held that an individual has no right to challenge a subpoena issued against the third-party bank. New York law precludes an individual's motion to quash a subpoena seeking the production of the individual's bank records directly from the third-party bank as the defendant lacks standing.⁵ (*People v Doe*, 96 AD2d 1018 [1st Dept 1983]; *People v DiRaffaele*, 55 NY2d 234 [1982]). In *United States v Miller*, (425 US 435 [1976]), the United States Supreme Court held that the bank records of a customer's accounts are "the business records of the banks," and that the customer "can assert neither ownership nor possession" of those records. In New York, the Appellate Division held that, "[b]ank records, although they reflect transactions between the bank and its customers, belong to the bank. The customer has no proprietary or possessory interests in them. Hence, he cannot preclude their production." (*People v Doe* at 1018).

Here, the defendant has no proprietary interests in the @destructuremal account's user information and Tweets between September 15, 2011 and December 31, 2011. As briefly mentioned before, in order to use Twitter's services, the process of registering an account requires a user's agreement to Twitter's Terms. Under Twitter's Terms it states in part:

By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed). (See <https://twitter.com/tos>).

In order to register the @destructuremal account, the defendant had to have agreed to those very same terms. Every single time the defendant used Twitter's services the defendant was granting a license for Twitter to use, display and distribute the defendant's Tweets to anyone and for any purpose it may have. Twitter's license to use the defendant's Tweets means that the Tweets the defendant posted were not his. The defendant's inability to preclude Twitter's use of his Tweets demonstrates a lack of proprietary interests in his Tweets.

⁴ In an unpublished short form order (Docket No. SUCR2011-11308), on February 23, 2012, the Suffolk Superior Court ordered Twitter to comply with the District Attorney of Suffolk County's administrative subpoena. Available at: http://aclum.org/sites/all/files/legal/twitter_subpoena/suffolk_order_to_twitter_20120223.pdf

⁵ The same principle has been applied to the records of a telephone company relating to an individual's account. (*Smith v Maryland*, 442 US 735 [1979])

This court finds that defendant's contention that he has privacy interests in his Tweets to be understandable, but without merit. Part of the Terms agreement reads: "The Content you submit, post, or display will be able to be viewed by other users of the Services and through third party services and websites." The size of the potential viewing audience and the time it can take to reach that audience is also no secret, as the Terms go on to disclose:

What you say on Twitter may be viewed all around the world instantly . . . [t]his license is you authorizing us to make your Tweets available to the rest of the world and to let others do the same.
(See <https://twitter.com/tos>).

Another section within Twitter's Terms notifies its users of Twitter's Privacy Policy, which governs the collection and use of any information a user provides to Twitter. Most significantly, the Privacy Policy lays out what Twitter's services are designed to do. It is "primarily designed to help you share information with the world . . ." because, "[m]ost of the information you provide . . . is information you are asking [Twitter] to make public." (See <http://twitter.com/privacy>). This information consists of more than just a user's Tweets, it also includes: "the lists you create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information." (See <http://twitter.com/privacy>).

As a result, public Tweets are even searchable by many search engines.⁶ At the heart of Twitter are small and rapid bursts of information that can contain a whole lot more than a 140 character long Tweet.⁷ Users' Tweets are what makes Twitter an information network that has the ability to reach out to people in nearly every country in the world.

In *Matter of Norkin v Hoey*, (181 AD2d 248, 253 [1st Dept 1992]), the Appellate Division held that, "there have been manifestations of an underlying discomfort with the facial unfairness of depriving a bank customer of any recourse, including standing, for disclosure of financial information concerning the customer's personal bank accounts which are widely believed to be confidential." Like bank records, user information and Tweets can contain sensitive personal information. With a

⁶ "About Public and Protected Tweets", available at: <https://support.twitter.com/groups/31-twitter-basics/topics/113-online-safety/articles/14016-about-public-and-protected-tweets>

⁷ Hence Twitter's official mascot, Larry . . . an embodiment of the idea of small and rapid "chirps" or bursts of information.

click of the mouse or now with even the touch of a finger, Twitter users are able to transmit their personal thoughts, ideas, declarations, schemes, pictures, videos and location, for the public to view. The widely believed (though mistaken) notion that any disclosure of a user's information would first be requested from the user and require approval by the user is understandable, but wrong. While the Fourth Amendment provides protection for our physical homes, we do not have a physical "home" on the Internet. What an Internet user simply has is a network account consisting of a block of computer storage that is owned by a network service provider. As a user, we may think that storage space to be like a "virtual home," and with that strong privacy protection similar to our physical homes. However, that "home" is a block of ones and zeroes stored somewhere on someone's computer. As a consequence, some of our most private information is sent to third parties and held far away on remote network servers. A Twitter user may think that the same "home" principle may be applied to their Twitter account. When in reality the user is sending information to the third party, Twitter. At the same time the user is also granting a license for Twitter to distribute that information to anyone, any way and for any reason it chooses. In *United States v Lifshitz*, (369 F3d 173 [2d Cir 2004]), the Second Circuit held that individuals do not have a reasonable expectation of privacy in internet postings or e-mails that have reached their recipients. "Users would logically lack a legitimate expectation of privacy in materials intended for publication or public posting" (*Id.* at 190 *citing Guest v Leis*, 255 F3d 325, 333 [6 Cir 2001]).

While a Twitter account's user information and Tweets contain a considerable amount of information about the user, Twitter does not guarantee any of its users complete privacy. Additionally, Twitter notifies its users that their Tweets, on default account settings, will be available for the whole world to see. Twitter also informs its users that any of their information that is posted will be Twitter's and it will use that information for any reason it may have. The @destructuremal account's Tweets were, by definition public. The defendant had knowledge that Twitter was to instantly distribute his Tweets to Twitter users and non-Twitter users, essentially anyone with Internet access. Indeed, that is the very nature and purpose of Twitter. Accordingly, this Court finds that the defendant has no standing to move to quash the subpoena.

2. DEFENDANT'S MOTION TO INTERVENE

The defendant moves to intervene in proceedings to quash the People's subpoena in the event that his direct standing to challenge the subpoena was denied.

The defendant argues that CPLR §1012 gives him the right to intervene, "when the representation of the person's interest is or may be inadequate and the person is or may be bound by the judgment." The defendant contends that his interest is not protected because of Twitter's inaction and defendant would be bound by any judgment allowing the subpoenaed information to be delivered to the District Attorney. The defendant also argues that pursuant to CPLR §1013, common questions of law and fact as to the legality of the subpoena, what the subpoena seeks for production, and the proper use of and procedure to obtain the records sought, are present by the defendant's claims in his motion to quash and the lack of a motion to quash by Twitter.

The People argue that CPLR §§ 1012 and 1013 do not apply to this case, as the defendant will not be bound by the enforcement of the subpoena on a third party. They also argue that the action seeking the enforcement of the subpoena on Twitter does not share any common question of law or fact with the defendant's disorderly conduct charge.

The Court finds that the defendant does not have intervention as of right. CPLR § 1012(a) states, "Upon timely motion, any person shall be permitted to intervene in any action . . . (2) when the representation of the person's interest by the parties is or may be inadequate and the person is or may be bound by the judgment . . ." In *Vantage Petroleum, Bay Isle Oil Co. v Board of Assessment Review of Town of Babylon*, (61 NY2d 695 [1984]), the Court of Appeals specifically ruled that an applicant for intervention is "bound" by a judgment in an action, only when a judgment would be *res judicata* as against the applicant. While the defendant's interests may not be adequately represented because of Twitter's inaction, it is clear that the defendant will not be bound by any of the principles of *res judicata* by any ruling in regards to the People's subpoena. The defendant cannot be bound by the ruling granting the production of information that the People's subpoena seeks, because he is not a party and not in privity with any party in the underlying action. (*Tyrone G. v Fifi N.*, 189 AD2d 8 [1st Dept 1993]). There is no "judgment" per se as well, the People have not submitted a plenary action seeking a final judgment. (*People v Thain*,

24 Misc 3d 377 [Sup Ct, NY County 2009]). This ruling is only to enforce the People’s subpoena served upon Twitter.

CPLR § 1013 states that, “Upon timely motion, any person may be permitted to intervene in any action when a statute of the state confers a right to intervene in the discretion of the court, or when the person’s claim or defense and the main action have a common question of law or fact. In exercising its discretion, the court shall consider whether the intervention will unduly delay the determination of the action or prejudice the substantial rights of any party.” The court will not exercise its discretion to permit the defendant to intervene pursuant to CPLR § 1013. The defendant’s arguments lacks any authority to justify the notion that he has a right to challenge the subpoena because the information sought may adversely affect him. “. . . [s]uch a broad and liberal rule would frustrate the very purpose of any investigation for such investigations always adversely affect someone and would not be necessary if they didn’t.” (*Matter of Selesnick*, 115 Misc 2d 993, 995 [Sup Ct, Westchester County 1982]).

Accordingly, the defendant’s motions are denied. However, it should be noted that during oral arguments the People consented to allow the materials to be produced to the court for *in camera* inspection.

THE STORED COMMUNICATIONS ACT

While this court holds that the defendant has no standing to challenge the subpoena as issued, once the subpoena is brought to a courts attention, it is still compelled to evaluate the subpoena under federal laws governing internet communications.⁸ The privacy of stored Internet communications in the United States is governed by the Stored Communications Act (“SCA”)(*See* 18 USC §§2701 - 2711) which was enacted in 1986 as part of the Electronic Communications Privacy Act (Pub.L. No 99-508, 100 Stat 1848).⁹

⁸ If asked to “so order” a subpoena it would be this court’s responsibility to make sure the subpoena is “legal,” relevant and not overbroad. Therefore, since the impact of this decision is to “so order” the People’s subpoena in this case, this court must evaluate the subpoena in such a manner.

⁹ *See*, Kerr, Orin S., “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending it” 72 GEO WASH L REV 1208

The statute creates rights held by “customers” and “subscribers” of network service providers in both content and noncontent information held by two particular types of providers. In order to evaluate the legality of the subpoena¹⁰, you must first classify the network service provider to see if the provider provides “electronic communication service,” “remote computing service,” or neither. Next, classify whether the information sought is the information content “in electronic storage,” content held by a remote computing service, a non-content record pertaining to a subscriber, or other information enumerated by the SCA. Then the court must consider whether the government is seeking to compel disclosure or seeking to accept information disclosed voluntarily by the provider.

If you look at the purpose and method of Twitter, it is clear to this court that Twitter is a service provider of electronic communication. The information sought by the prosecutor in this case has been discussed previously. It is also clear that they are seeking to compel Twitter to provide this information.

The SCA permits the government to compel disclosure of the basic subscriber and session information listed in 18 U.S.C. § 2703(c)(2) using a subpoena:

(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)
(*See* 18 USC § 2703[c][2]).

The legal threshold for issuing a subpoena is low. (*See United States v Morton Salt Co.*, 338 US 632, 642-43 [1950]). Prosecutors may obtain disclosure using any federal or state grand jury or

¹⁰ *See also*, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,” Published by The Computer Crime and Intellectual Property Section Criminal Division of The U.S. Dep’t of Justice, available at: <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.

trial subpoena or an administrative subpoena authorized by a federal or state statute (18 USC § 2703[c][2]).

To obtain any of the following, the prosecutor must either give notice or seek a ninety day delay of notice¹¹:

- 1) everything that can be obtained using a subpoena without notice;
- 2) “the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days.” 18 USC § 2703(a); and
- 3) “the contents of any wire or electronic communication” held by a provider of remote computing service “on behalf of . . . a subscriber or customer of such remote computing service.” (18 USC § 2703[b][1][B][i]), § 2703[b][2).

In this case, the subpoena adhered to all of the SCA’s pertinent provisions. The People’s subpoena is authorized by CPL § 610.10 and therefore, under 18 USC § 2703(c)(2), it may compel disclosure of the basic user information that the subpoena seeks.

¹¹ 18 USC § 2705(a)(1)(B) permits notice to be delayed for ninety days “upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result.”

This court order will also compel Twitter to disclose @destructuremal account's Tweets, pursuant to 18 USC § 2703(d). In order to obtain the court order found in § 2703(d), the People must offer "specific and articulable facts showing that there are reasonable grounds to believe" that the Tweets "are relevant and material to an ongoing criminal investigation." (18 USC § 2703[d]). This court finds that the factual showing has been made. In the response to the defendant's motion, the People state that the information sought by the subpoena is needed to refute the defendant's anticipated defense, that the police either led or escorted the defendant into stepping onto the roadway of the Brooklyn Bridge. The People claim the defendant's anticipated defense is contradicted by his public statements,¹² which identifies the @destructuremal account as likely belonging to the defendant and indicates that while on the Brooklyn Bridge the defendant may have posted Tweets that were inconsistent with his anticipated trial defense.

This court holds that this hearing and the notice given to the defendant by Twitter clearly gave the defendant notice of what the prosecutor was doing.¹³ The account holder clearly exercised his option¹³ to contest the subpoena in this case, and while the court ultimately has decided that the defendant does not have standing to quash the subpoena, the court has reviewed the subpoena and the court file to determine that there is in fact reasonable grounds to believe that the information sought was relevant and material to this investigation. Additionally, the court does not believe that the subpoena was overbroad in its request. Moreover, any privacy concerns of the defendant will be balanced and protected by the *in camera* review of the materials sought.

Accordingly, it is hereby:

¹² See, Harris, Malcolm, "I'm the Jerk Who Pranked Occupy Wall Street," available at: <http://gawker.com/5868073>; see also, "A Bridge to Somewhere," available at: <http://thenewinquiry.com/essays/a-bridge-to-somewhere/>

¹³ This court declines to opine on whether the actions of Twitter to unilaterally decide to give notice to the account holder may be in violation of state or federal laws.

ORDERED, that Twitter comply with the January 26, 2012 subpoena that was previously served on their offices within twenty days of receipt of this order; and it is further

ORDERED, that the materials be provided to this court for *in camera* inspection. The relevant portions thereof will be provided to the office of the District Attorney, who will provide copies to the defense counsel as part of discovery; and it is further

ORDERED, that The Clerk of this Court notify the Presiding Judge of Jury 7 of the receipt of the materials.

This opinion shall constitute the decision and order of the Court.

Dated: April 20, 2012

New York, New York

Matthew A. Sciarrino, Jr.
Judge of the Criminal Court