**People v Harris** 2012 NY Slip Op 22175 [36 Misc 3d 868] June 30, 2012

Sciarrino Jr., J. Criminal Court Of The City Of New York, New York County

Published by New York State Law Reporting Bureau pursuant to Judiciary Law § 431. As corrected through Tuesday, October 23, 2012

**Criminal Court of the City of New York, New York County, June 30, 2012**

APPEARANCES OF COUNSEL

*Perkins Coie*, Washington, D.C. (*John K. Roche* of counsel), and *Perkins Coie*, New York City (*Jeffrey D. Vanacore* of counsel), for Twitter, Inc., movant. *Cyrus R. Vance, Jr., District Attorney*, New York City (*Lee Langston* of counsel), for plaintiff. *Martin R. Stolar*, New York City, for defendant. *Aden J. Fine*, New York City, *Marcia Hofmann* and *Hanni Fakhoury*, San Francisco, California, and *Paul Alan Levy*, Washington, D.C., for American Civil Liberties Union and another, amici curiae.

{**36 Misc 3d at 869} OPINION OF THE COURT

Matthew A. Sciarrino, Jr., J.

Twitter, Inc. (Twitter) seeks to quash the January 26, 2012 subpoena issued by the New York County District Attorney's{**36 Misc 3d at 870} Office and upheld by this court's April 20, 2012 order. That order required Twitter to provide any and all user information, including email addresses, as well as any and all tweets posted for the period of September 15, 2011 to December 31, 2011, from the Twitter account @destructuremal, which was allegedly used by Malcolm Harris. This is a case of first impression, distinctive because it is a criminal case rather than a civil case, and the movant is the corporate entity (Twitter) and not an individual (Harris). It also deals with tweets that were publicly posted rather than an email or text that would be directed to a single person or a select few.

On October 1, 2011, the defendant, Malcolm Harris, was charged with disorderly conduct (Penal Law § 240.20 [5]) after allegedly marching on the roadway of the Brooklyn Bridge. On January 26, 2012, the People sent a subpoena duces tecum to Twitter seeking the defendant's account information and tweets for their relevance in the ongoing criminal investigation (CPL art 610; 18 USC § 2703 [c] [2]). On January 30, 2012, Twitter, after conferring with the District Attorney's Office, informed the defendant that the Twitter account @destructuremal had been subpoenaed. 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 the court ruled on the defendant's motion to quash the subpoena and intervened.

On April 20, 2012, this court held that the defendant had no proprietary interest in the user information on his Twitter account, and he lacked standing to quash the subpoena (*see* CPLR 1012 [a]; 1013; *People v Harris*, 36 Misc 3d 613 [Crim Ct, NY County 2012]). This court ordered Twitter to provide certain information to the court for in camera review to safeguard the privacy rights of Mr. Harris.

On May 31, 2012, David Rosenblatt, a member of Twitter's Board of Directors, was personally served within New York County with a copy of this court's April 20, 2012 order, a copy of the January 26, 2012 trial subpoena, and a copy of the March 8, 2012 trial subpoena. Twitter subsequently moved to quash the April 20, 2012 court order. To date, Twitter has not complied with this court's order.

## Discussion

Twitter is a public, real-time social and information network that enables people to share, communicate, and receive news. {**36 Misc 3d at 871} Users

can create a Twitter profile that contains a profile image, background image, and status updates called tweets, which can be up to 140 characters in length on [*2]the website.[FN1] Twitter provides its services to the public at large. Anyone can sign up to use Twitter's services as long as they agree to Twitter's terms. Twitter is a Delaware corporation with its principal place of business in California.

The Stored Communications Act (SCA) (18 USC § 2701 *et seq.*) defines and makes distinctions between electronic communication service (ECS) versus remote computing service (RCS), and content information versus non-content information. ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." (*See* 18 USC § 2510 [15].) RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." (*See* 18 USC § 2711 [2].) The Wiretap Act (18 USC § 2510 *et seq*.) defines content information as follows: "contents, when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." (18 USC § 2510 [8].) In contrast, logs of account usage, mailer header information (minus the subject line), lists

of outgoing email addresses sent from an account, and basic subscriber information are all considered to be non-content information.[FN2]

While Twitter is primarily an ECS (as discussed in *Harris*, 36 Misc 3d at 621-622), it also acts as an RCS. It collects and stores both non-content information such as IP addresses, physical locations, browser type, subscriber information, etc. and content information such as tweets. The SCA grants greater privacy protections to content information because actual contents of messages naturally implicate greater privacy concerns than network generated information about those communications.[FN3]

1. Twitter Users and Standing to Challenge Third-Party Disclosure Requests

Twitter argues that users have standing to quash the subpoena. The issue is whether Twitter users have standing to{**36 Misc 3d at 872} challenge third-party disclosure requests under the terms of service that existed during the dates in question. In *Harris* (36 Misc 3d at 623), the New York City Criminal Court held that a criminal defendant did not have standing to quash a subpoena issued to a third-party online social networking service because the defendant has no proprietary interest. The court's decision was partially based on Twitter's then terms of service agreement. After the April 20, 2012 decision, Twitter

changed its terms and policy effective May 17, 2012. The newly added portion states: "You Retain Your Right To Any Content You Submit, Post Or Display On Or Through The Service." (*See* Twitter, *Terms of Service*, http://twitter.com/tos/ [accessed June 11, 2012].)

[*3]Twitter argues that the court's decision to deny the defendant standing places an undue burden on Twitter. It forces Twitter to choose between either providing user communications and account information in response to all subpoenas or attempting to vindicate its users' rights by moving to quash these subpoenas itself. However, that burden is placed on *every* third-party respondent to a subpoena (*see In re Verizon Internet Servs., Inc.*, 257 F Supp 2d 244, 257-258 [2003]; *United States v Kennedy*, 81 F Supp 2d 1103, 1110 [2000]) and cannot be used to create standing for a defendant where none exists.

The Stored Communications Act (18 USC § 2703 [d]) states: "A court issuing an order pursuant to this section, on a motion made promptly by *the service provider, may quash or modify such order*, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." (Emphasis added.)

In the defense motion they also reference a concurrence by Justice Sotomayor who said that "it may be necessary [for the court] to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (*see United States v Jones*, 565 US —, —, 132 S Ct 945, 957 [2012]). Publication to third parties is the issue. Tweets are not emails sent to a single party. At best, the defense may argue that this is more akin to an email that is sent to a party and carbon copied to hundreds of others. There can be no reasonable expectation of privacy in a tweet sent{**36 Misc 3d at 873} around the world.[FN4] The court order is not unreasonably burdensome to Twitter, as it does not take much to search and provide the data to the court.[FN5] So long as the third party is in possession of the materials, the court may issue an order for the materials from the third party when the materials are relevant and evidentiary (18 USC § 2703 [d]; *People v Carassavas*, 103 Misc 2d 562 [Saratoga County Ct 1980]).

Consider the following: a man walks to his window, opens the window, and screams down to a young lady, "I'm sorry I hit you, please come back upstairs." At trial, the People call a person who was walking across the street at the time this occurred. The prosecutor asks, "What did the defendant yell?" Clearly the answer is relevant and the witness could be compelled to testify. Well today, the

street is an online, information superhighway, and the witnesses can be the third-party providers like Twitter, Facebook, Instragram, Pinterest, or the next hot social media application. [*4]

2. The Court Order, Federal Law and New York State Law

The second issue is whether the court order was a violation of the Fourth Amendment, the Federal Stored Communications Act, or any other New York law.

The Fourth Amendment

To establish a violation of the Fourth Amendment, the defendant must show either (1) a physical intrusion onto defendant's personal property, or (2) a violation of a defendant's reasonable expectation of privacy. (*See United States v Jones*, 565 US —, —, 132 S Ct 945, 950 [2012]; *Kyllo v United States*, 533 US 27, 33 [2001].) In *Jones* (565 US at —, 132 S Ct at 949), the U.S. Supreme Court held that the government's installation of a Global Positioning System (GPS) tracking device on a target's vehicle to obtain information was a physical intrusion on a constitutionally protected area. In *People v Weaver* (12 NY3d 433 [2009]), the New York Court of Appeals held that the placing of a GPS tracking device inside the bumper of the defendant's {**36 Misc 3d at 874} vehicle, by a

state police investigator, was a physical intrusion. However, in this case there was no *physical* intrusion into the defendant's Twitter account. The defendant had purposely broadcasted to the entire world into a server 3,000 miles away. Therefore, the defendant's account is protected by the Fourth Amendment *only* if "the government violate[d] a subjective expectation of privacy that society recognizes as reasonable." (*See Kyllo v United States*, 533 US 27, 33 [2001], citing *Katz v United States*, 389 US 347, 361 [1967].)[FN6]

The Supreme Court has repeatedly held that the Fourth Amendment does not protect information revealed by third parties. (*See United States v Miller*, 425 US 435, 443 [1976].) Several courts have applied this rationale and held that Internet users do not retain a reasonable expectation of privacy. In *Romano v Steelcase Inc.* (30 Misc 3d 426, 433 [Sup Ct, Suffolk County 2010]) the court held that "users would logically lack a legitimate expectation of privacy in materials intended for publication or public posting."[FN7]

If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist.

[*5]Those private dialogues would require a warrant based on probable cause in order to access the relevant information.

Interestingly, in 2010, Twitter signed an agreement with the Library of Congress providing that every public tweet from Twitter's inception and beyond would be archived by the{**36 Misc 3d at 875} Library of Congress.[FN8] Also, Twitter's privacy policy states in part:

> "Our Services are primarily designed to help you share information with the world. Most of the information you provide us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Services." (*See* Twitter, *Twitter Privacy Policy*, https://twitter.com/privacy [accessed June 11, 2012].)

There is no reasonable expectation of privacy for tweets that the user has made public. It is the act of tweeting or disseminating communications to the public that controls. Even when a user deletes his or her tweets there are search engines available such as "Untweetable," "Tweleted" and "Politwoops" that hold users accountable for everything they had publicly tweeted and later deleted.[FN9]

Therefore, the defendant's Fourth Amendment rights were not violated because there was no physical intrusion of the defendant's tweets and the

defendant has no reasonable expectation of privacy in the information he intentionally broadcasted to the world.

Stored Communications Act

The SCA's requirements for a court order state that

> "[a] court order for disclosure under subsection (b) or (c) . . . shall issue only if the governmental entity offers specific and articulate facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or {**36 Misc 3d at 876} *the records or other information sought, are [*6]relevant and material to an ongoing criminal investigation*" (*see* 18 USC § 2703 [d] [emphasis added]).

The defendant's anticipated trial defense is that the police either led or escorted him onto the non-pedestrian part of the Brooklyn Bridge, a defense allegedly contradicted by his publicly posted tweets around the time of the incident. In *Harris* (36 Misc 3d at 623), the court held that the information sought was relevant. The April 20, 2012 court order was issued to comply with the January 26, 2012 subpoena.

The People are seeking two types of information, non-content information such as subscriber information, email addresses, etc. and content information such as tweets. The SCA protects only private communications[FN10] and allows disclosure of electronic communication when it is not overbroad.[FN11]

In general, court orders have no limitations on the types of information to be disclosed (18 USC § 2703 [d]). The SCA mandates different standards that the government must satisfy to compel a provider to disclose various types of information (18 USC § 2703). To compel a provider of ECS to disclose the contents of communication in its possession that are in temporary "electronic storage" for 180 days or less, the government must obtain a search warrant (18 USC § 2703 [a]). A court order must be issued to compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose its contents (18 USC § 2703 [a], [b], [d]). The law governing compelled disclosure also covers the above-mentioned non-content records. The rules are the same for providers of ECS and RCS and the government can obtain a section 2703 (d) order to compel such non-content information (18 USC § 2703 [c] [1] [B]).

The non-content records such as subscriber information, logs maintained by the network server, etc. and the September 15,{**36 Misc 3d at 877} 2011 to December 30, 2011 tweets are covered by the court order. However, the government must obtain a search warrant for the December 31, 2011 tweets.

[*7]New York State Law

The scope of a subpoena duces tecum is sufficiently circumscribed when: (1) the materials are relevant and evidentiary; (2) the request is specific; (3) the materials are not otherwise procurable reasonably in advance of trial by the exercise of due diligence; (4) the party cannot properly prepare for trial without such a production and inspection in advance of trial and the failure to obtain such inspection may tend unreasonably to delay the trial; and (5) the application is made in good faith and is not intended as a general "fishing expedition" (*People v Carassavas*, 103 Misc 2d 562, 564 [1980], citing *People v Price*, 100 Misc 2d 372, 379 [1979]). The District Attorney seeks the subpoenaed information to refute Harris's anticipated trial defense. In *Harris* (36 Misc 3d at 623), the court agreed that the subpoena duce tecum was sufficiently circumscribed and a court order was issued on April 20, 2012 to comply with the subpoena.

On May 31, 2012, David Rosenblatt, a member of Twitter's Board of Directors, was personally served within New York County with a copy of this court's April 20, 2012 order, a copy of the January 26, 2012 trial subpoena, and a copy of the March 8, 2012 trial subpoena. There are no jurisdictional issues and there are no violations of the New York Constitution.

## Conclusion

In dealing with social media issues, judges are asked to make decisions based on statutes that can never keep up with technology.[FN12] In some cases, those same judges have no understanding of the technology themselves (Stephanie Rabiner, Esq., Technologist, *Do Judges Really Understand Social Media?*, http://blogs.findlaw.com/technologist/2012/05/do-judges-really-understand-social-media.html [May 9, 2012]). Judges must then do what they have always done—balance the arguments on the scales of justice. They must weigh the interests of society against the inalienable rights of the individual who gave away some rights when entering into the social contract that created our government and the laws that we have agreed to follow. {**36 Misc 3d at 878} Therefore, while the law regarding social media is clearly still developing, it can neither be said that this court does not understand or appreciate the place that social media has in our society nor that it does not appreciate the importance of this ruling and future rulings of courts that may agree or disagree with this decision. In recent years, social media has become one of the most prominent methods of exercising free speech, particularly in countries that do not have very many freedoms at all.

The world of social media is evolving, as is the law around it. Society struggles with policies, whether they are between student and teacher (New York City Department of Education, NYC Department of Education Social Media Guidelines),[FN13] or the right of a company to examine an applicant's Facebook page as part of the interview process (Bill Chappell, *State Approves Bill to Ban Employers From Seeking Facebook Login Info*, http://www.npr.org/blogs/thetwo-way/2012/04/10/150354579/state-[*8]approves-bill-to-ban-employers-from-seeking-facebook-login-info). As the laws, rules and societal norms evolve and change with each new advance in technology, so too will the decisions of our courts. While the U.S. Constitution clearly did not take into consideration any tweets by our founding fathers, it is probably safe to assume that Samuel Adams, Benjamin Franklin, Alexander Hamilton and Thomas Jefferson would have loved to tweet their opinions as much as they loved to write for the newspapers of their day (sometimes under anonymous pseudonyms similar to today's Twitter user names). Those men, and countless soldiers in service to this nation, have risked their lives for our right to tweet or to post an article on Facebook; but that is not the same as arguing that those public tweets are protected. The Constitution gives you the right to post, but as numerous people have learned, there are still consequences for your public

posts. What you give to the public belongs to the public. What you keep to yourself belongs only to you.

Accordingly, the motion to quash is granted in part and denied in part. The court finds in favor of the People for all non-content information and content information in ECS and RCS from September 15, 2011 to December 30, 2011. However, ECS content information less than 180 days old (tweeted on Dec. 31, 2011) may only be disclosed pursuant to a search warrant, and{**36 Misc 3d at 879} the court decision in *People v Harris* is so modified. That search warrant should be requested of a judge of competent jurisdiction. However, to avoid any issue of alleged non-impartiality, that warrant should be made to another judge of this court.

Accordingly, it is hereby: ordered, that Twitter disclose all non-content information and content information from September 15, 2011 to December 30, 2011; 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 2 of the receipt of the materials.

## Footnotes

**Footnote 1:** *See* Twitter, *Guidelines for Law Enforcement*, https://support.twitter.com/entries/41949-guidelines-for-law-enforcement/ (accessed May 30, 2012).

**Footnote 2:** Orin Kerr, *A User's Guide to the Stored Communications Act, and the Legislator's Guide to Amending It*, 72 Geo Wash L Rev 1208 (2004).

**Footnote 3:** 36 Misc 3d at 622.

**Footnote 4:** In fact, on August 1, 2012 your tweets will be sent across the universe to a galaxy far, far away (*see* Chris Taylor, Mashable Social Media, *Your Tweets to Be Beamed Across Space. Will ET RT?*, http://mashable.com/2012/06/26/et-rt/ [June 26, 2012]).

**Footnote 5:** The general New York rule is that only the recipient of a subpoena in a criminal case has standing to quash it (*see People v Lomma*, 35 Misc 3d 395, 404-405 [Sup Ct, NY County 2012], citing *People v Doe*, 96 AD2d 1018, 1019 [1st Dept 1983] [banking and telephone records], and *People v Crispino*, 298 AD2d 220, 221 [1st Dept 2002] ["defendant, as a customer, has no proprietary interest" in the defendant's bank account records]).

**Footnote 6:** See also *People v Suleman* (NYLJ 1202499796548 [Crim Ct, NY County, June 22, 2011]) where the court held that the taxicab owner had no reasonable expectation of privacy of the information generated and stored by a GPS device in the cab.

**Footnote 7:** Twitter argues that the court should embrace the holding in *United States v Warshak* (631 F3d 266 [6th Cir 2010]). In *Warshak*, the court found that the defendant had a reasonable expectation of privacy in his emails. However, the *Warshak* case is distinguishable from the case at hand because the former deals with private emails as opposed to public postings. *Warshak* did not address public communications at all; instead the court held only that "email requires

strong protection under the Fourth Amendment" (*Warshak*, 631 F3d at 286). If such Fourth Amendment protections were to extend to *public* postings, it would undermine the very basis of the *Warshak* holding.

**Footnote 8:** (*See* Matt Raymond, Library of Congress, *How Tweet It Is!: Library Acquires Entire Twitter Archive*, http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/ [accessed May 30, 2012].) The Twitter community received the initial heads up via their own feed @librarycongress. Twitter has its users' consent for disclosure to the Library of Congress by virtue of its privacy policy. The Library of Congress' archives are not yet available due to its high volume of composition of billions of tweets, and with an estimate of 140 million new tweets per day. (*See* Audrey Watters, *How the Library of Congress is Building the Twitter Archive*, http://radar.oreilly.com/2011/06/library-of-congress-twitter-archive.html [accessed June 11, 2012].)

**Footnote 9:** *See* http://untweetable.com; http://tweleted.com/; http://mashable.com/2012/05/30/politwoops/.

**Footnote 10:** *See Kaufman v Nest Seekers, LLC*, 2006 WL 2807177, *5, 2006 US Dist LEXIS 71104, *15-16 (SD NY 2006) (only electronic bulletin boards which are not readily accessible to the public are protected under the SCA); *Konop v Hawaiian Airlines, Inc.*, 302 F3d 868, 875 (9th Cir 2002) ("The legislative history of the [Electronic Communications Protection Act] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards"); *Snow v DirecTV, Inc.*, 450 F3d 1314, 1320-1321 (11th Cir 2006) (holding that the SCA does not apply to material that is readily available to the public).

**Footnote 11:** Orin Kerr, *A User's Guide to the Stored Communications Act, and the Legislator's Guide to Amending It*, 72 Geo Wash L Rev 1208 (2004).

**Footnote 12:** The SCA was enacted in 1986 and mainly applied to the start of emails. The SCA was enacted long before the creation of Twitter and the concept of blogging which started in 2006.

**Footnote 13:**
Http://schools.nyc.gov/NR/rdonlyres/BCF47CED-604B-4FDD-B752-DC2D81504478/0/DOESocialMediaGuidelines20120430.pdf