TOURO LAW
Touro College Jacob D. Fuchsberg Law Center

Touro Law Review

Volume 29
Number 4 *Annual New York State Constitutional Issue*

Article 16

March 2014

Privacy in Social Media: To Tweet or Not to Tweet?

Tara M. Breslawski

Privacy in Social Media: To Tweet or Not to Tweet?

Cover Page Footnote
29-4

PRIVACY IN SOCIAL MEDIA: TO TWEET OR NOT TO TWEET?

COURT OF APPEALS OF NEW YORK

People v. Harris[1]
(decided June 30, 2012)

I. FACTUAL BACKGROUND

During the Occupy Wall Street movement, Malcolm Harris participated in a protest march on the Brooklyn Bridge.[2] During this protest march, Harris, along with others, was arrested and charged with disorderly conduct for marching on the roadway of the bridge, as opposed to the pedestrian walkway.[3] As part of the investigation, the District Attorney's office sought to acquire Harris's Twitter records through a subpoena.[4] The District Attorney's office had reason to believe that the information contained in these Twitter records would contradict his anticipated defense at trial.[5] Twitter notified Harris that his account had been subpoenaed.[6] Harris moved to quash the subpoena based on the privacy rights afforded by the Fourth Amendment[7] and the rules set forth in the Stored Communications Act.[8] Twitter subsequently stated that it would not comply with the subpoena until the motion to quash was ruled on.[9]

The court first addressed the issue of Harris's standing to quash the subpoena in an April 2012 hearing.[10] Although the issue

---

[1] 949 N.Y.S.2d 590 (Crim. Ct. 2012).

[2] People v. Harris, 945 N.Y.S.2d 505, 506 (Crim. Ct. 2012).

[3] *Id.* (noting that Harris had the option of remaining on the pedestrian walkway and obeying the law, but chose to step off onto the roadway along with other protesters).

[4] *Id.*

[5] *Id.* at 512.

[6] *Id.* at 506.

[7] U.S. CONST. amend. IV.

[8] 18 U.S.C. §§ 2701-2712 (2006).

[9] *Harris*, 945 N.Y.S.2d at 507.

[10] *Id.*

has not been raised in the context of social networking, courts have repeatedly held that a defendant does not have standing to quash a subpoena issued to third party banks.[11] Similarly, Harris had no proprietary interest in his Twitter account information or tweets.[12] When Harris signed up to use Twitter's services, he agreed to "grant[] a license for Twitter to use, display, and distribute the defendant's Tweets to anyone and for any purpose it may have."[13] Twitter also explicitly informs its users that, through the default settings, tweets may be viewed by the entire world and that information posted may be used by Twitter for any reason.[14] Harris did in fact have an account that allowed his tweets to be viewed publicly, and thus, was on notice that anyone with Internet access could view, print out, or use these tweets in any way.[15] Without this proprietary interest, Harris had no standing to quash the subpoena.[16]

Following this ruling, the court decided that the subpoena issued to Twitter for Harris's account and tweets was not overbroad and sought relevant investigatory information, and thus, it compelled Twitter to comply with the subpoena.[17] However, Twitter then sought to quash the subpoena itself and once again refused to comply with the court order to turn over the requested information.[18] In a June 2012 hearing, Twitter argued that the court based its conclusion about Harris's lack of standing on the "Terms of Service" that was in effect at the time the tweets were posted.[19] After the April decision was handed down, Twitter changed its policy to include a section stating "You Retain Your Right To Any Content You Submit, Post Or Display On Or Through The Service,"[20] thus creating a proprietary interest for Harris in his tweets. Although Twitter argued that denying the defendant standing to quash the subpoena places a bur-

---

[11] *Id.* at 507-08.

[12] *Id.* at 508.

[13] *Id.* (noting that the license meant the tweets were not property of the defendant).

[14] *Harris*, 945 N.Y.S.2d at 509-10 ("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.").

[15] *Id.* at 510.

[16] *Id.*

[17] *Id.* at 512-13.

[18] *Harris*, 949 N.Y.S.2d at 591-92.

[19] *Id.* at 593.

[20] *Id.* (citing Twitter, *Terms of Service*, https://twitter.com/tos/ (last modified June 25, 2012)) (internal quotation marks omitted).

den on Twitter to comply with all subpoenas or to move to quash subpoenas on behalf of all defendants, the court found that every third party service bears this burden and an exception would not be made for Twitter.[21] The court also refused to accept Twitter's argument that the court should follow the holding in *United States v. Warshak*.[22] In *Warshak*, the Court held that a person retains a reasonable expectation of privacy in his or her emails; however, the court in *Harris* reasoned that *Warshak* is distinguishable because the emails in *Warshak* were private communications, whereas the tweets in *Harris* were posted on a public forum, the Internet, and therefore the tweets were undeserving of the same protection.[23]

The court in *Harris* ultimately decided that the subpoena issued to Twitter complied with the statutory requirements to compel disclosure of both the account information and the tweets publicly posted from September 15, 2011 to December 30, 2011.[24] On the other hand, the court concluded that the tweets from December 31, 2011 could only be discovered pursuant to a warrant.[25] This however, was not, and still is not, the end of the story for *Harris*.

II. HISTORICAL OVERVIEW

Centuries ago, inhabitants of the United States were granted protections from governmental searches through the United States Constitution and its Fourth Amendment. For the most part, this "right to privacy" only extended to the enumerated list as set out in the Amendment. Electronic communications are obviously not listed in this amendment because when our forefathers drafted the Constitution, electronic communication was unimaginable. Thomas Jefferson did not think that someday he would be able to update his Facebook status to "Just finished writing the first article of the Constitution! All right!" or that George Washington would tweet to James Madison, "I hope they finish this Constitution soon, I just want to be President already! #USA."[26] As the technology individuals have at their finger-

[21] *Id.*

[22] 631 F.3d 266 (6th Cir. 2010).

[23] *Harris*, 949 N.Y.S.2d at 595 n.7.

[24] *Id.* at 598.

[25] *Id.* The reasons for this distinction will be discussed later in the analysis of the federal statutes governing this issue. *Infra* section IV.

[26] The "#" symbol is referred to as a hashtag on Twitter and is used to denote a keyword or phrase in a tweet. The term or phrase that follows the hashtag can be searched on Twitter

tips today is beyond anything our founding fathers would have ever thought possible, statutes enacted by the legislature and judicial interpretations of the Fourth Amendment are the only ways to protect such electronic communications.

The government's response to this modern-day upsurge in the use of technology and electronic communications was the Stored Communications Act ("SCA").[27] This Act provides different protections for information transmitted and stored electronically. This distinction is determined based upon whether the information is stored on an electronic communication service provider or a remote computing service provider and whether the information contained is content or non-content. These distinctions and the privacy provided will be discussed in length later in this case note.

In addition to the protection the Fourth Amendment and the SCA provide to electronic communications, websites that provide a platform to relay information electronically (especially social media websites) often have their Terms of Use[28] and Privacy Policy[29] laid out on their website. Twitter, for example, has both of these listed on its website, as well as Guidelines for Law Enforcement.[30] These policies inform users as to what content and information can be provided to the government voluntarily, and what information requires a court order, such as a subpoena.

Similar to Twitter, Facebook and MySpace are social media websites where people can update their statuses to share what they are thinking or doing, share other personal information, or upload photographs and videos of themselves and others.[31] All three of these social networking sites allow users to control their privacy settings in order to monitor who can see certain information that they have shared.[32] The basic assumption of these social media websites is that in creating an account, the user implicitly consents to sharing his information with others, regardless of the self-regulated privacy set-

---

and all other tweets using that keyword are shown. *Harris*, 945 N.Y.S.2d at 506 n.1.

[27] 18 U.S.C. §§ 2701-2712 (2006).

[28] Twitter, *Twitter Terms of Service*, https://twitter.com/tos (last modified June 25, 2012).

[29] Twitter, *Twitter Privacy Policy*, https://twitter.com/privacy (last modified May 17, 2012).

[30] Twitter Help Center, *Guidelines for Law Enforcement*, https://support.twitter.com/articles/41949-guidelines-for-law-enforcement (last visited Aug. 8, 2012).

[31] Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 653 (Sup. Ct. 2010).

[32] *Id*. at 654.

tings.[33] One court has stated that it is blatantly unreasonable for a person who voluntarily signed up for an account on a website, and voluntarily chose to post and disclose information on the site, to then claim that he is owed Fourth Amendment privacy protection to that content.[34] While, centuries ago, a person may have yelled something out the window to someone on the street and that statement could have been used against the yeller by any passerby who heard it, "today, the street is an online, information superhighway, and the witnesses can be the third party providers like Twitter, Facebook, Instragram [sic], Pinterest, or the next hot social media application."[35] Thus, whether in a street or social media context, the information has been disseminated to the public, which dissipates the reasonable expectation of privacy.

III. THE FOURTH AMENDMENT'S APPLICATION TO REASONABLE EXPECTATIONS OF PRIVACY

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[36]

In many cases involving Fourth Amendment violations, courts have reiterated the well-established precedent, observing that this amendment was intended to protect the privacy of a *person* and not a *place*.[37] The United States Supreme Court has established that the sphere of protected privacy is not all encompassing, but rather, the expectation of privacy must be reasonable.[38] This is usually where

---

[33] *Id.* at 657 ("Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.").

[34] *Id.* at 656 ("The privacy concerns are far less where the beneficiary herself chose to disclose the information.") (quoting Beye v. Horizon Blue Cross Blue Shield N.J., No. 06-5337, 2007 WL 7393489, at *1, *2 n.3 (D.N.J. Dec. 14, 2007)).

[35] *Harris*, 949 N.Y.S.2d at 594.

[36] U.S. CONST. amend. IV.

[37] *See Romano*, 907 N.Y.S.2d at 655; *see also* Katz v. United States, 389 U.S. 347, 351 (1967).

[38] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first

the private-versus-public battle begins. Is a statement made or an action done in the public eye subject to Fourth Amendment protections?

A pivotal case concerning the privacy afforded to electronic communications was addressed by the United States Supreme Court in *Katz v. United States*.[39] There, federal agents had reason to believe the defendant was transmitting illegal gambling bets over the phone in a public telephone booth.[40] The agents subsequently attached an electronic listening device to the outside of the telephone booth and used the information obtained to form the basis for his conviction.[41] The defendant argued that this electronic eavesdropping constituted a search under the Fourth Amendment and because it was done without a warrant, it violated his rights.[42] The Court agreed.[43] In this decision, the Court formulated the aforementioned mantra that "the Fourth Amendment protects people, not places."[44] The Court reasoned that if a person knowingly exposes something to the public, he is therefore abandoning any privacy right he might have otherwise retained and is no longer protected by the Fourth Amendment.[45] Likewise, absent precautions taken to preserve the reasonable expectation of privacy, an individual consequently forfeits this constitutional protection.[46] However, as the Court also stated, not everything exposed to or occurring in the public is without Fourth Amendment protection.[47]

In *Kyllo v. United States*,[48] the Court resolved an issue with regard to more advanced forms of surveillance technology, addressing the Fourth Amendment implications underlying the use of a thermal imaging device to detect levels of heat in a private home.

---

that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' ").

[39] 389 U.S. 347 (1967).

[40] *Id.* at 348.

[41] *Id.*

[42] *Id.*

[43] *Id.* at 353 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").

[44] *Katz*, 389 U.S. at 351.

[45] *Id.*

[46] *Id.* at 361 (Harlan, J. concurring).

[47] *Id.* at 351.

[48] 533 U.S. 27 (2001).

The Department of the Interior Agents were suspicious that the defendant was growing marijuana in his home.[49] Based on their experience and expertise, the agents knew marijuana growth in a home would require high-intensity lamps.[50] In order to determine if such lamps were being used inside the defendant's home, the agents used a thermal-imaging device on a public street, aimed at the private home.[51] The device detected high heat areas of the house, which allowed the agents to establish probable cause to acquire a warrant to enter and search the home.[52] When the defendant contested the constitutionality of the warrant and search in court, the Court found that because a thermal-imaging device is not in general public use, and the information obtained from the device would not have been discovered by the naked eye, the use of the technology constituted a search and was subject to Fourth Amendment protection.[53] This protection would require the agents to procure a warrant before using the device.[54] The Court's ruling in *Kyllo* was similar to that in *Katz*, establishing that there need not be a physical intrusion in order to constitute a search that is protected by the Fourth Amendment.[55]

A recent issue in regard to electronic communication is the legality of tracking individuals through the use of global positioning systems ("GPS") on vehicles, and whether this constitutes a search under the Fourth Amendment.[56] One might think that a person voluntarily thrusts their vehicle into the public eye when they drive it along a road, and therefore, the exterior of the car is not subject to a reasonable expectation of privacy.[57] However, is a simple visual surveillance team that follows the suspect car equivalent to the information that can be provided by around the clock monitoring through GPS signals?

The landmark case involving privacy issues related to the use

---

[49] *Id.* at 29.

[50] *Id.*

[51] *Id.* at 29-30.

[52] *Id.* at 30.

[53] *Kyllo*, 533 U.S. at 40.

[54] *Id.* (noting that the warrant was only obtained after the device was used).

[55] *Id.*

[56] For an in depth analysis of the Fourth Amendment implications of GPS tracking devices see United States v. Jones, 132 S. Ct. 945 (2012) and People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009).

[57] *Jones*, 132 S. Ct. at 952 (quoting New York v. Class, 475 U.S. 106, 114 (1986)).

of a GPS tracking device was *United States v. Jones*.[58] In *Jones*, agents believed that the defendant was involved in trafficking narcotics.[59] In order to investigate this suspicion, agents applied for a warrant to install a GPS device on his vehicle.[60] The defendant's vehicle was tracked for 28 days, which allowed the agents to collect enough information to indict him on drug related charges.[61] However, in *Jones*, the Supreme Court disagreed with the Court's reasoning in *Katz* that would lead one to believe that there is no reasonable expectation of privacy for a car that is traveling on a public road.[62] Rather, the Court found that installing a device that provided around the clock surveillance over a four-week period constituted a search.[63]

Thus, courts must determine whether using modern technology to enhance human senses during a search triggers Fourth Amendment protection. A person may choose to keep many aspects of his life private, such as the places frequented or the company kept.[64] The electronic signals given off by the GPS monitor may be more intrusive than simply following a car (which would not require a warrant to be constitutional). A surveillance team introduces inherent human error, such as the possibility that the team may lose track of the car's location. This is a factor that a person is deprived of when a GPS monitor is attached to his vehicle, and thus, privacy is decreased through the use of such technology.

A Third Party Disclosure

To ultimately determine the amount of privacy that should be afforded, courts need to determine the intrusiveness and general availability of electronic communications, and also need to consider a user's voluntary disclosure to third parties during the normal use of

---

[58] 132 S. Ct. 945 (2012).

[59] *Id.* at 947.

[60] *Id.*

[61] *Id.*

[62] *Id.* at 950-52 (citing *Class*, 475 U.S. at 114) (noting that the use of the *Katz* reasoning would mean no search occurred because an owner of a car would have no expectation of privacy when traveling on public roads, as he or she would be visible to all).

[63] *Jones*, 132 S. Ct. at 949.

[64] *Id.* at 955 (Sotomayor, J., concurring). "Disclosed in [GPS] data . . . will be trips to the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Weaver*, 909 N.E.2d at 1199.

the technologies. In *United States v. Miller*,[65] the defendant was convicted of defrauding the national whiskey tax.[66] For evidence to support these charges, the government subpoenaed his financial records from a bank.[67] The Court found that these records were admissible and did not violate the defendant's Fourth Amendment rights because he "can assert neither ownership nor possession. Instead, these are the business records of the banks."[68] As the Court in *Miller* recognized, the United States Supreme Court has repeatedly held that when information is voluntarily conveyed to a third party and the third party subsequently is compelled by authorities to disclose this information, there is no Fourth Amendment violation.[69] There is no reasonable expectation of privacy in information that is voluntarily conveyed to a third party, such as a bank, telephone company, or host website. This voluntary third party disclosure to host websites was addressed in the New York case, *Romano v. Steelcase, Inc*.,[70] which is discussed in greater detail later in this case note.

B Social Media as Virtual Homes?

Information, thoughts, photographs, and videos posted on a personal social media site must be stored somewhere for the user, or others whom the user chooses to share this information with, to access it at the click of a mouse. This user may believe he has a "virtual home," but in reality, his information is retained in "a block of computer storage that is owned by a network service provider."[71] Because many users believe that this information is being held in their "virtual home," it is a common misconception that this storage area should be afforded the same privacy protections that a physical home receives under the Fourth Amendment.[72] This belief is greatly unrealistic because in these instances, a user's private information must be sent to a third party to be held on its network server.[73] The reality is that every status update or tweet sent to Facebook or Twit-

---

65 425 U.S. 435 (1976).
66 *Id.* at 436.
67 *Id.*
68 *Id.* at 440.
69 *Id.* at 443.
70 907 N.Y.S.2d 650 (Sup. Ct. 2010).
71 *Harris*, 945 N.Y.S.2d at 509.
72 *Id.*
73 *Id.*

ter, respectively, whether posted on a public or private account, is never really private; all of this information must be sent to and stored with the third party host (in this example, Facebook and Twitter). The question then turns to whether users have a reasonable expectation of privacy in their information, even though it has been shared with a host third party.

Recently, there has been a surge in litigation regarding the privacy afforded to the perceived "virtual home." In *In re § 2703(d) Order*,[74] the prosecution sought information regarding Twitter accounts that were under investigation by the government in connection with Wikileaks.[75] The court explicitly stated that it was "aware of no authority finding that an IP address shows location with precision, let alone provides insight into a home's interior or user's movements."[76] Therefore, any "virtual home" privacy is in direct contrast with the privacy afforded to the actual home, as in *Katz* and *Kyllo*.[77] Because the Twitter users voluntarily allowed Twitter to collect their IP addresses, the court held that the idea of a "virtual home" holding a privacy expectation was invalid.[78]

The "virtual home" concept was further discussed in two federal cases, *Tompkins v. Detroit Metro. Airport*[79] and *Howell v. Buckeye Ranch*,[80] which resolved issues relating to the privacy afforded to sections of a social media account deemed "private" as opposed to "public." In *Tompkins*, the court stated that information that is on a "private" social media page "that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy."[81] Similarly, the court in *Howell* held that "relevant information in the private section of a social media account is

---

[74] 787 F. Supp. 2d 430 (E.D. Va. 2011).

[75] *Id.* at 435.

[76] *Id.* at 440.

[77] *Id.*

[78] *Id.*

[79] No. 10-10413, 2012 U.S. Dist. LEXIS 5749, at *1 (E.D. Mich. Jan. 18, 2012).

[80] No. 11-CV-1014, 2012 U.S. Dist. LEXIS 141368, at *1 (S.D. Ohio Oct. 1, 2012).

[81] *Tompkins*, 2012 U.S. Dist. LEXIS 5749, at *4. In the omitted footnote, the court explicitly states that it is not addressing the issue of whether there is a reasonable expectation of privacy in a "private" social media page consistent with the Fourth Amendment, nor whether a search warrant or a statutory subpoena is required to obtain the information located on that page. *Id.* n.1.

discoverable."[82] Both of these decisions included limiting dicta to the effect that the request for the information contained on a social media page cannot be overbroad and must only seek information that is relevant to the ongoing case.[83] Nonetheless, in essence, these cases opened the door for authorities to further invade the "virtual home" and even request information that a person made an effort to keep out of the public view and away from prying eyes. However, this is not a free-for-all for law enforcement, as statutory provisions will guide the way to the proper disclosure of electronic communication.

IV. FEDERAL APPROACH: THE STORED COMMUNICATIONS ACT

In 1986, the legislature enacted the SCA as part of the Electronic Communications Privacy Act ("ECPA").[84] As previously mentioned, although the Fourth Amendment provides strong privacy protection for our physical homes, it does not offer the same refuge for our "virtual homes."[85] The SCA was enacted mainly as a gap-filler for the areas of our electronic lives that we would like to remain private, but which were not offered any previous protection.[86] Anytime law enforcement officers are seeking electronic information, such as email, subscriber information, or any other record of a user, from a service provider, the officer must comply with the provisions set forth by the SCA.[87] When looking into what the SCA does or does not protect, each electronic communication must be analyzed to see which category it falls into, which controls the applicable level of

---

[82] *Howell*, 2012 U.S. Dist. LEXIS 141368, at *2 (citing Glazer v. Fireman's Fund Ins. Co., No. 11-CV-4374, 2012 WL 11997167, at *1, *3-*4 (S.D.N.Y. April 5, 2012)).

[83] *See Tompkins*, 2012 U.S. Dist. LEXIS 5749, at *7; *Howell*, 2012 U.S. Dist. LEXIS 141368, at *2-*3.

[84] *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (discussing the protections granted to electronic data by the SCA and the guidelines for complying with the Act). The Electronic Communications Privacy Act also included the Pen/Trap Statute, 18 U.S.C. §§ 3121-27 (2006), which "governs the interception of the noncontent associated with communications," and the Wiretap Statute, 18 U.S.C. §§2510-22 (2006), which "governs the interception of communications content in transit." THOMAS K. CLANCY, CYBERCRIME AND DIGITAL EVIDENCE: MATERIALS AND CASES 257 (Lexis Nexis, 2011). Neither of those statutes have any application to the case at hand.

[85] Kerr, *supra* note 84, at 1209-10 ("Although a user may think of that storage space as a 'virtual home,' in fact that 'home' is really just a block of ones and zeroes stored somewhere on somebody else's computer" and it is this transfer to a third party that removes the privacy right from the user's communication.").

[86] *Id*. at 1210.

[87] CLANCY, *supra* note 84, at 269.

privacy protection.[88]

The amount of privacy that should be afforded to postings on social media sites is a topic that many professionals, scholars, and even judges[89] have a difficult time understanding. Because all of the information posted on these networking sites is a form of electronic communication under the SCA, it is important to first break down the different storage areas in which a communication may be retained,[90] and then describe the differences between content or non-content communication stored within a system. An "electronic communication service" ("ECS") is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[91] A common example of this type of system is a computer copying emails and storing them pending their delivery.[92] There is an obvious privacy concern with this type of service in that private, personal emails are sent, without direction by the user, to a third party for temporary storage on an outside network computer.[93] A "remote computing service" ("RCS") is defined quite differently as "the provision to the public of computer storage or processing services by means of an electronic communications system."[94] In other words, a company may pay a public provider to have remote computers store or process a large amount of information that their in-house computers may not be able to retain or handle.[95] Similar to an ECS, the pri-

---

[88] The United States Department of Justice has identified three steps to help determine what is protected by the SCA.

> First, they must classify the network service provider [as ECS, RCS, or neither]. . . . Next they must classify the information sought [as content or non-content]. . . . Third, they must consider whether they are seeking to compel disclosure [through a "search warrant, a 2703(d) court order, or a subpoena"] or seeking to accept information disclosed voluntarily by the provider.

CLANCY, *supra* note 84, at 272.

[89] Rabiner, Stephanie, Esq., Technologist, *Do Judges Really Understand Social Media?* http://blogs.findlaw.com/technologist/2012/05/do-judges-really-understand-social-media.html (last visited Aug. 8, 2012).

[90] *See* CLANCY, *supra* note 84, at 287-88 for a thorough example set forth by the Department of Justice of the SCA classifications.

[91] 18 U.S.C. § 2510 (15) (2006).

[92] Kerr, *supra* note 84, at 1213 (noting that the copies created by the provider may stay on the provider's computer for many months, thus susceptible to privacy concerns).

[93] *Id.*

[94] 18 U.S.C. § 2711(2) (2006).

[95] Kerr, *supra* note 84, at 1213-14. Non-public providers of RCS are not protected under the SCA. CLANCY, *supra* note 84, at 273.

vacy concern implicated by an RCS is also that the private information is being sent to a third party and is often retained by that third party for a significant amount of time.[96] Content information is statutorily defined "with respect to any wire, oral, or electronic communication, [to] include[ ] any information concerning the substance, purport, or meaning of that communication."[97] For instance, in Harris's case, the actual text of the tweet would be considered content information.[98] This is information that a user chooses to write, post, and share with others on Twitter.[99] Non-content information is classified as basic subscriber information, such as logs of account usage, and in the case of Twitter, lists of others who follow the user and in turn the user himself is following.[100] The SCA's statutory standards provide more privacy for content information than non-content information because the substance of an electronic communication is usually what a user seeks to protect.

In order for the SCA to preserve privacy interests of customers or subscribers, the relevant part of the statute addresses the rules the government must follow when seeking to compel the disclosure of communications and records.[101] Section 2703 provides in pertinent part as follows:

> A government entity may require the disclosure by a provider *of electronic communication service* of the *contents* of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued . . . by a court of competent jurisdiction.[102]
>
> A governmental entity may require a provider of *re-*

---

[96] Kerr, *supra* note 84, at 1214.

[97] 18 U.S.C. § 2510(8) (2006).

[98] *Harris*, 949 N.Y.S.2d at 596.

[99] Kerr, *supra* note 84, at 1228 (noting that the example of content used here is the body of an email—the actual text that someone wrote and intended to send to a specified recipient).

[100] *Id.* (providing another email example, additional non-content information is the "mail header information minus the subject line" and "lists of outgoing e-mail addresses sent from an account").

[101] *Id.* at 1218.

[102] 18 U.S.C. § 2703(a) (2006) (emphasis added) (noting that in order to obtain the contents of a wire or electronic communication that has been stored in an electronic communication system for more than one hundred and eighty days, the same method as obtaining information from a remote computing service must be utilized).

> *mote computing service* to disclose the *contents* of any wire or electronic communication . . . without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued . . . by a court of competent jurisdiction; or with prior notice from the governmental entity to the subscriber or customer if the governmental entity uses an administrative subpoena . . . or obtains a court order . . . .[103]

The relevant part of the SCA that governs the disclosure of *non-content* records provides:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (*not including the contents of the communication*) only when the governmental entity obtains a warrant . . . ;[104] obtains a court order . . . ;[105] has the consent of the subscriber or customer to such disclosure;[106] . . . or a provider of electronic communication service or remote computing servicer shall disclose to a governmental entity the name, address, local and long distance telephone connection records, or records or session times and durations; length of service (including state date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service. . . of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).[107]

The final part to the relevant statute under the SCA states the requirements for the government to seek a court order to compel the

---

[103] 18 U.S.C. § 2703(b) (2006).
[104] 18 U.S.C. § 2703(c)(1)(A) (2006).
[105] 18 U.S.C. § 2703(c)(1)(B) (2006).
[106] 18 U.S.C. § 2703(c)(1)(C) (2006).
[107] 18 U.S.C. § 2703(c)(2) (2006) (emphasis added).

disclosure of *content* information. This section provides:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[108]

To summarize these statutory provisions, the privacy protections afforded to electronic communications through the SCA have been described as an "upside down pyramid" and the "higher up in the pyramid you go, the more information the government can obtain."[109] At the bottom (or the smallest part of the pyramid), the SCA only requires a subpoena to obtain basic subscriber information from a service.[110] Moving up the pyramid, the next step is a § 2703(d) order that allows the government to obtain non-content records.[111] Next, a subpoena, along with prior notice, allows the government access to basic subscriber information, permanently held files, and contents in temporary electronic storage for more than 180 days.[112] Going even further up the pyramid is a § 2703(d) order coupled with prior notice, which allows the government to acquire all non-content records, any permanently held files, and contents in temporary electronic storage for more than 180 days.[113] Finally, at the top of the pyramid (or the widest part), a search warrant is sufficient for the government to compel everything that is stored in an account.[114]

Applying this understanding of the SCA to the case at hand,

---

[108] 18 U.S.C. § 2703(d) (2006).

[109] Kerr, *supra* note 84, at 1222.

[110] *Id*. This subscriber information generally includes name, address, network address, phone number, etc. CLANCY, *supra* note 84, at 291.

[111] Kerr, *supra* note 84, at 1222. The 2703(d) order requires "specific and articulable facts demonstrating reasonable grounds to believe that the [records] are relevant and material to an ongoing criminal investigation" in order to be granted. CLANCY, *supra* note 84, at 291 (internal quotation marks omitted).

[112] Kerr, *supra* note 84, at 1222-23.

[113] *Id*. at 1223 ("Put another way, a 2703(d) order plus prior notice compels everything except contents in temporary 'electronic storage' 180 days or less.").

[114] *Id.* This search warrant includes disclosure of content information stored for 180 days or less and does not require prior notice. CLANCY, *supra* note 84, at 291.

Twitter is mainly an ECS, but also has functions of an RCS.[115] Furthermore, Twitter collects and maintains non-content information, including "IP addresses, physical locations, browser type, [and] subscriber information," as well as content information including tweets.[116] If the District Attorney's office had issued a search warrant to Twitter, the officials would have had access to all of the information, non-content and content, stored in Harris's account. However, because only a subpoena was served, the discoverable information was slightly limited.[117]

V. THE NEW YORK APPROACH

In accord with the lack of clear precedent in the federal courts, New York courts have not definitively defined the sphere of privacy afforded to what a person posts on their social media website.[118] For guidance, the courts have looked to the New York Constitution, which is very similar to the United States Constitution. Although the textual language of the relevant section offers no greater protection to electronic communications than the Fourth Amendment, as a general rule, New York courts grant individuals greater privacy rights.[119]

In *People v. Hall*,[120] the court turned to federal statutes to analyze the extent of privacy protections in electronic information.[121]

---

[115] *Harris*, 949 N.Y.S.2d at 593.

[116] *Id.*

[117] *Id.* at 596 (noting that the tweets from December 31, 2011 required a search warrant for disclosure).

[118] *Romano*, 907 N.Y.S.2d at 656.

[119] *Weaver*, 909 N.E.2d at 1207-1208 (Read, J., dissenting) ("Interpretive review essentially flows from textual differences between a provision of the State Constitution and its federal counterpart, and is not available here since the operative language of the Fourth Amendment and article I, section 12 is the same."); Article I, section 12 of the New York Constitution states identical language to the Fourth Amendment and provides:

> The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated, and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable ground to believe that evidence of crime may be thus obtained, and identifying the particular means of communication, and particularly describing the person or persons whose communications are to be intercepted and the purpose thereof.

N.Y. CONST. art. I, § 12.

[120] 823 N.Y.S.2d 334 (Sup. Ct. 2006).

[121] *Id.* at 338.

The SCA guidelines for the government compelling disclosure of electronic communications apply in state courts just the same as they would in federal courts. In *Hall*, government agents obtained cell phone records from T-Mobile to determine the location from which individual defendants had placed calls after a shooting had occurred.[122] The defendant sought to suppress the information received, arguing that the subpoena requesting the records was issued without probable cause and violated his constitutional rights.[123] Hall conceded that the government complied with the SCA guidelines requiring specific facts to be stated to prove the information sought was relevant to an ongoing investigation, but argued that the cell phone was used as a tracking device, thus violating the Electronic Communication Privacy Act of 1986.[124] This act provides that even though a device is not specifically created to track a person, it may be considered a tracking device if it is used in that manner.[125] Neither the United States Constitution nor the New York Constitution provide a means to determine the protection that should be afforded to individuals, limiting use of this electronic device, so the court in *Hall* chose to look at the ECPA. In turn, the court found that because the cell phone records were only sought to determine a general location of the defendants at a specified time *and* that this information was a product of normal use of the cell phone, it was not used as a "tracking device," and thus, did not violate the ECPA.[126] The court in *Hall* also discussed the third party disclosure issue and compared the records kept by T-Mobile during its normal course of business to that of the bank records in *Miller* and the pen register in *Maryland v. Smith.*[127] As a result, the New York court's ruling in *Hall* was consistent with the federal trend of finding that an individual does not have an expectation of privacy in information collected and retained by someone else.[128]

In the next major electronic tracking case in New York State, *People v. Weaver*,[129] the court explained that it was solely following

---

[122] *Id.* at 337.

[123] *Id.* at 335.

[124] *Id.* at 338 ("Under the ECPA the People must seek prior court approval based upon probable cause, before they may use a 'tracking device.' ").

[125] *Hall*, 823 N.Y.S.2d at 339.

[126] *Id.* at 341.

[127] *Id.* at 342.

[128] *Id.*

[129] 909 N.E.2d 1195 (N.Y. 2009).

the protections afforded under the New York Constitution because the federal law was not definitive on the issue of electronic communications.[130] Similar to the federal case on point, *Jones*, agents in *Weaver* placed a GPS tracking device on a vehicle and tracked it for 65 days, eventually using the information obtained to charge the defendant with two burglaries.[131] The court in *Weaver* reasoned that, though GPS technology has become widespread for various uses, this does not mean that a person's privacy has been virtually taken away.[132] Ultimately, the court found that the use of the device required a warrant based on probable cause under the New York Constitution, absent exigent circumstances.[133] Even though this case was decided in New York based solely on its state constitution, the similarities in the text of both the Fourth Amendment and the relevant section of the New York Constitution allowed this decision to lay the foundation for *Jones*, which would be heard in the federal system three years later.

The first case in New York to address the privacy concerns raised in social media and electronic communication contexts was *Romano v. Steelcase*.[134] The court's ruling in *Romano* built off of the federal precedent established in the Second and Sixth Circuits, recognizing that "[u]sers would logically lack a legitimate expectation of privacy in materials intended for publication or public posting."[135] In *Romano*, the plaintiff claimed that she had suffered physical and mental injuries, and in order to refute the actual extent of those injuries, the defendants sought access to Romano's social media accounts.[136] These accounts were arguably relevant because they contained pictures of the plaintiff enjoying a normal and active lifestyle after the accident, contrary to her claims.[137] The court granted permission to view these profiles based on the inherent public nature of them and the previous voluntary disclosure of the information to the

---

[130] *Id.* at 1202.

[131] *Id.* at 1195-96.

[132] *Id.* at 1200 ("Here, particularly, where there was no voluntary utilization of the tracking technology, and the technology was surreptitiously installed, there exists no basis to find an expectation of privacy so diminished as to render constitutional concerns de minimis.").

[133] *Id.* at 1203.

[134] 907 N.Y.S.2d 650 (Sup. Ct. 2010).

[135] *Id.* at 656.

[136] *Id.* at 651.

[137] *Id.* at 652 ("Plaintiffs who place their physical condition in controversy, may not shield from disclosure material which is necessary to the defense of the action.").

third party host site.[138]

Most recently, the Fourth Department of the Supreme Court, Appellate Division addressed the privacy afforded to social media in *Kregg v. Maldonado*.[139] In *Kregg*, the plaintiff's son was in an accident while driving a Suzuki motorcycle.[140] The defendants sought to have social media websites, including Facebook and MySpace, which maintained accounts set up by the family on behalf of the injured son, disclose the "entire contents" of those accounts.[141] The court reasoned that, "[a]lthough CPLR 3101(a) provides for 'full disclosure of all matter material and necessary in the prosecution or defense of an action,' it is well settled that a party need not respond to discovery demands that are overbroad."[142] The court endeavored to prevent discovery from becoming a "fishing expedition" by denying the defendants' request to gain full access to individuals' social media accounts.[143]

After deciding whether the electronic information at issue is afforded privacy protection or is discoverable, New York courts require that the discovering party obtain a subpoena to compel the production of the discoverable material. By court order, a party may attain a subpoena duces tecum in order to compel a person or company to appear and produce the specific records requested.[144] New York courts have defined the preliminary requirements to warrant an issuance of this type of subpoena as:

> (1) [T]he 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 production and the 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

---

[138] *Id*. at 656 ("The privacy concerns are far less where the beneficiary herself chose to disclose the information.") (quoting *Beye*, 2007 WL 7393489 at *1, *2 n.3).

[139] 951 N.Y.S.2d 301 (App. Div. 4th Dep't 2012).

[140] *Id.* at 301-02.

[141] *Id.* at 302.

[142] *Id.* (citing N.Y. C.P.L.R. § 3101(a) (McKinney 2011)).

[143] *Id*. at 302 (noting that a party should not be allowed to search a person's entire account in hopes that it will contain evidence relating to or rebutting the claimed injuries).

[144] N.Y. C.P.L.R. § 2301 (McKinney 2011).

is not intended as a general "fishing expedition."[145]

As previously noted, a subpoena is only effective to gain access to basic subscriber information and communications that have been stored and designated as permanently held files. As long as prosecutors follow the specified rules set out in the statute, a user who posts information on a social media site that can be viewed publicly is not afforded an additional safe haven for privacy under the New York Constitution.

VI. CONCLUSION

It is inevitable that technology is moving forward at a greater pace than the laws that are needed to govern its impact. Social networking is on the rise not only for personal use, such as to keep in touch with family and friends, but also for companies to reach out to potential customers and consumers. Social media sites have also become an integral part of many background checks and interview processes for new or potential employees.[146] While it might be said that our founding fathers figuratively fought for our right to post status updates on Facebook and tweet whatever we choose, their fight did not provide an accompanying guarantee that the content would remain private.[147] With the sole purpose of social networking sites being to *share information with others*, it seems almost counterintuitive to think that a user would believe that this information was not destined for public viewing.[148] Although it may seem like allowing government officials to have unlimited access to the information stored in a social media account is like allowing them to read a person's diary, sometimes a certain amount of disclosure is necessary in order to assist an ongoing criminal investigation and ensure justice is served.

As previously stated, in *Harris*, the court enforced the rules established by the SCA and in turn denied the motion to quash in part and granted it in part.[149] Because the information sought was requested through a subpoena, the stored electronic communications

---

[145] *Harris*, 949 N.Y.S.2d at 596.

[146] *Id.* at 597.

[147] *Id.*

[148] *Id.* at 597-98 ("What you give to the public belongs to the public. What you keep to yourself belongs only to you.").

[149] *Id*. at 598.

that were over 180 days old were appropriately compelled.[150] However, a search warrant was required to lawfully obtain the one day of information that was sought that was less than 180 days old.[151] Since that hearing in June, Twitter has been putting up quite a fight on behalf of Harris's privacy rights. Twitter appealed the denial of the motion to quash and consequently refused to turn over the tweets that were lawfully subpoenaed.[152] The judge handling the case threatened to hold Twitter in contempt if it did not turn over the records because Twitter's resistance was causing undue delay in bringing the case to trial.[153] Subsequently, Twitter moved for a stay of all proceedings until its appeal on the motion to quash was heard.[154] The court found that until it came to decision on that motion, the stay was not yet in effect, and thus, Twitter must turn over the subpoenaed records and tweets in order to avoid a contempt finding that comes with a hefty fine.[155] Twitter begrudgingly complied with the demand with a promise from the judge that the information would not be viewed until there was a ruling on the stay.[156]

In today's techno-centric world, people should be aware that almost anything and everything that they say or do may be recorded on some medium. No matter how hard a person may try to delete something, it still exists somewhere out in cyberspace and can be found by anyone who wants to take the time to look for it.[157] So the next time you go to update your Twitter account, think of the potential consequences of the content you're posting, and ask yourself, to tweet or not to tweet?

---

[150] *Harris*, 949 N.Y.S.2d at 598.

[151] *Id.*

[152] Andrew Keshner, *D.A. Seeks to Doom Twitter's Bid to Stay Review of Tweets*, N.Y.L.J., Sept. 7, 2012.

[153] *Id.*

[154] *Id.*

[155] Christine Simmons, *Twitter Is Given a Deadline to Avoid Contempt Finding*, N.Y.L.J., Sept. 12, 2012.

[156] Christine Simmons, *Twitter Reluctantly Turns Over Documents of Occupy Protester*, N.Y.L.J., Sept. 17, 2012.

[157] *Harris*, 949 N.Y.S.2d at 595 ("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.").

Tara M. Breslawski[*]

[*] Touro Law, J.D. Candidate (2014); Western New England College, B.S.C.J. (2011). Special Thanks: To my parents, who have provided me with unconditional love and support over the years and always pushed me to pursue my dreams. To Alexander DePalo for being a shoulder to lean on through thick and thin. To Dean Fabio Arcila, Jr. for his guidance on this case note and for the constant reminder to always think critically. To the members of the *Touro Law Review*, especially Danielle M. Hansen, for their guidance and advice throughout this process.