

 Tweet

0

Share

0

SOCIAL MEDIA EVIDENCE IN CRIMINAL PROCEEDINGS: AN UNCERTAIN FRONTIER

By Justin P. Murphy and Adrian Fontecilla, [Crowell & Moring's Washington](#)

Social media has evolved into a fundamental pillar of communication in today's society, revolutionizing how the world does business, learns about and shares news, and instantly engages with friends and family. Not surprisingly, this exploding medium significantly impacts government investigations and criminal litigation because social media factors into the majority of cases in some respect.

Social media evidence can include photographs, status updates, people's location at a certain time, and direct communications to a defendant's social media accounts, among others.

THE IMPORTANCE OF SOCIAL MEDIA

Most people use social media in their everyday lives. 91 percent of today's online adults use social media regularly, and "[s]ocial networking continues to reign as the top online activity."¹

Social media use in the United States alone has increased by 356 percent since 2006.² Currently, 52 percent of Americans have at least one social media profile,³ more than one billion people use Facebook actively each month,⁴ and Twitter has over 140 million active users posting 340 million Tweets a day.⁵

Every minute, social media users create massive amounts of data: Facebook users share 684,478 pieces of content; Tumblr blog owners publish 27,778 new posts; YouTube users upload 48 hours of new video; Foursquare users perform 2,083 check-ins; Flickr users add 3,125 new photos, and Instagram users share 3,600 new photos.⁶ In addition, there are hundreds of other social networking websites, each catering to a different demographic.⁷

The myriad and continually changing ways to share information via social media has resulted in a digital goldmine of potential evidence: profiles, lists of friends, group memberships, messages, chat logs, Tweets, photos, videos, tags, GPS locations, check-ins, login timetables and more.⁸

The information available from social media providers is staggering. When a phone company responds to a government subpoena or search warrant, it may provide call or message logs. In contrast, when a social media company such as Facebook responds to a government subpoena it provides the user's profile, wall posts, photos uploaded by the user, photos in which the user was

tagged, a comprehensive list of the user's friends with their Facebook IDs, and a long table of login and IP data.⁹

Moreover, with the advent of location-based services offered by social media companies like Facebook, Twitter, and FourSquare, precise location information will be increasingly maintained in the ordinary course of business and subject to the same subpoenas and search warrants.¹⁰ Not surprisingly, each social media subpoena can yield admissions or incriminating photos, among other evidence.¹¹

ACCESSING PUBLICLY AVAILABLE SOCIAL MEDIA EVIDENCE

It is no secret that government agencies mine social networking websites for evidence because, even without having to seek a warrant from the court or issue a subpoena, there are troves of social media evidence publicly available.¹² A majority of government agencies are active participants, contributing content and soliciting information through social media.¹³

Given the amount of information publicly available, and the avenues that the government has to seek out such information, the government often does not even need a search warrant, subpoena or court order to obtain social media evidence.

But, government agents can, and do, go further than defense counsel is allowed in pursuing social media evidence for a criminal proceeding. To bypass the need for a search warrant, government agents may pierce the privacy settings of a person's social media account by creating fake online identities or by securing cooperating witnesses to grant them access to information.¹⁴

In *(United States v. Meregildo)*,¹⁵ for example, the defendant set the privacy settings on his Facebook account so that only his Facebook "friends" could view his postings. The government obtained the incriminating evidence against the defendant through a cooperating witness who happened to be Facebook "friends" with the defendant.

The defendant moved to suppress the evidence seized from his Facebook account, arguing that the government had violated his Fourth Amendment rights. The court found:

SOCIAL MEDIA COMPANIES, SUBPOENAS, AND WARRANTS

Given the digital goldmine of potential evidence available from social media companies, it is not surprising that they are increasingly targeted by search warrants and government subpoenas in criminal matters.

For example, Twitter received more government requests for user information in the first half of 2012 than in the entirety of 2011.¹⁷ And over 80 percent of those requests were from authorities in the United States.¹⁸

Google, which is a provider of social networking sites like YouTube and Google+, has also seen an uptick in the frequency with which it receives subpoenas and search warrants in criminal matters. Statistics published by Google, which “primarily cover requests in criminal matters,”¹⁹ show that the number of Google user data requests received from government authorities in the United States increased more than 40 percent from 2009 to 2011.²⁰

Moreover, the prevalence of social media evidence in criminal proceedings will continue to proliferate as government agencies continue to formally train their personnel to search for and collect social media evidence.

A recent survey of over 1,200 federal, state, and local law enforcement professionals revealed that social media is widely used to assist in investigations, that few have received formal training on how to use social media for investigations, and that “74 percent of those not currently using it ... intend to start using it.”²¹

Furthermore, the case law is already replete with instances where the government obtained social media evidence through a warrant or subpoena directed at a social media company.²² Social media evidence is the new frontier of criminal proceedings, and it raises unique legal challenges, including issues of admissibility and a defendant's constitutional rights in material maintained by social media companies.

ACCOUNTING FOR THE STORED COMMUNICATIONS ACT

Federal law provides that, in some circumstances, the government may compel social media companies to produce social media evidence without a warrant. The Stored Communications Act (“SCA”) governs the ability of governmental entities to compel service providers, such as Twitter and Facebook, to produce content (e.g., posts and Tweets) and non-content customer records (e.g., name and address) in certain circumstances.²³

The SCA, which was passed in 1986, has not been amended to reflect society's heavy use of new technologies and electronic services, such as social media, which have evolved since the SCA's original enactment.²⁴

As a result, courts have been left to determine how and whether the SCA applies to the varying features of different social media services, applying precedent from older technologies such as text messaging pager services and electronic bulletin boards.²⁵

The SCA provides that non-content records can be compelled via a subpoena or court order.²⁶ Regarding compelled disclosure of the content of communications, the SCA provides different levels of statutory privacy protection depending on how long the content has been in electronic storage. The government may obtain content that has been in electronic storage for 180 days or less “only pursuant to a warrant.”²⁷

The government has three options for obtaining communications that have been in electronic storage with a service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d).²⁸

The constitutionality of the SCA has been called into question by at least one U.S. Circuit Court of Appeals. In *United States v. Warshak*, the Sixth Circuit held that “the government agents violated the Fourth Amendment when they obtained the contents of [defendant’s] emails” without a warrant, and added that “to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.”²⁹

The court reasoned that “[o]ver the last decade, email has become ‘so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification’” and that therefore “email requires strong protection under the Fourth Amendment.”³⁰

Noting that email was analogous to a phone call or letter and that the internet service provider was the intermediary that made email communication possible—the functional equivalent of a post office or telephone company—the court concluded that given “the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”³¹

As social media becomes as pervasive and important to people as email, its treatment under the SCA will require similar clarification by courts.

DEFINING A DEFENDANT’S CONSTITUTIONAL RIGHTS REGARDING SOCIAL MEDIA EVIDENCE

Courts have also begun to grapple with novel issues regarding the constitutionality of the government’s use of information obtained from social media companies in criminal proceedings.³²

For example, in November 2012, a New York appellate court heard arguments regarding Twitter’s appeal of two court orders in the prosecution of an Occupy Wall Street protestor.³³ The trial court held that the defendant lacked standing to move to quash the government’s third-party subpoena to Twitter for his account records and that his Tweets were not protected by the Fourth Amendment.³⁴ The trial court similarly denied Twitter’s motion to quash the government’s subpoenas for the defendant’s Twitter records for the same reasons, among others.³⁵

Notably, the defendant was only able to move to quash the subpoena because “Twitter’s policy is to notify users of requests for their information prior to disclosure,”³⁶ a policy which is becoming more common among social media companies.³⁷ Not only does Twitter notify its users that the company has received a government-issued information request for the user’s data, Twitter also protects its business by litigating against such third-party government subpoenas.³⁸

Twitter argued on appeal that the defendant has standing to quash the government's subpoena because he has a proprietary interest in his Tweets, pointing to the express language of Twitter's Terms of Service.³⁹

Moreover, Twitter argued that the defendant's Tweets are protected by the Fourth Amendment, primarily because the government concedes that the Tweets it sought were not made public by the defendant.⁴⁰ And, if a defendant has a reasonable expectation of privacy under the Fourth Amendment in his or her non-public emails,⁴¹ Twitter argued that not affording that same protection to users' non-public Tweets would create "arbitrary line drawing."⁴²

Finally, even assuming the Tweets in question were public, Twitter argued that the government still requires a search warrant under the Federal and New York constitutions.⁴³ Notwithstanding Twitter's pending appeal, Twitter complied with a court order requiring it to promptly submit the Defendant's Tweets under seal.⁴⁴

The line-drawing concerns expressed by Twitter in its *People v. Harris* brief— that a defendant's reasonable expectation of privacy under the Fourth Amendment in his or her social media records depends on the privacy settings for the particular account in question—were implicated in *United States v. Meregildo*, described above, where the Court held that "where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment."⁴⁵

Some courts have concluded that individuals have "a reasonable expectation of privacy to [their] private Facebook information and messages."⁴⁶

Those courts, while recognizing the importance of properly understanding how Facebook works, distinguished between a "private message" and a post to a user's Facebook wall.

Using privacy setting distinctions to determine social media users' constitutional rights may result in arbitrary line drawing that may evaporate as social media evolves.

Indeed, with Facebook's customizable and post-specific privacy settings, a person sharing a message by posting it on another user's wall can actually make it as private as information shared via a Facebook message.⁴⁷

In addition, it remains uncertain whether, given the sheer breadth of information available in any particular social media account, search warrants for entire social media accounts can be successfully challenged for lacking sufficient limits or boundaries that would enable the government-authorized reviewing agent to ascertain which information the agent is authorized to review.⁴⁸

Ultimately, because an expectation of privacy under the Fourth Amendment is partly a function of

whether “society [is] willing to recognize that expectation as reasonable,” social media’s rapid proliferation throughout today’s society may influence the privacy protections afforded to social media evidence in the future.⁴⁹

DEFENDING A CRIMINAL CASE WITH SOCIAL MEDIA EVIDENCE

Defendants face more significant obstacles than the government when seeking exculpatory evidence from social media companies.⁵⁰ First, defendants and their counsel do not share the government’s freedom to sleuth for publicly-available social media evidence.⁵¹ Ethics opinions issued to lawyers in various states have established that a defendant’s lawyer may not “friend” or direct a third person to “friend” another party or witness in litigation in order to search for impeachment material or exculpatory evidence.⁵²

Second, Defendants face additional hurdles when seeking to issue a third party subpoena.⁵³ Defendants may seek to subpoena social media companies for user information regarding the victim, the complaining witness, or another witness.⁵⁴

In those instances, in federal criminal proceedings, defendants must pursue such non-party discovery pursuant to [Federal Rule of Criminal Procedure 17](#) and seek a court order allowing such a subpoena.⁵⁵ Among other hurdles in seeking such an order, the court may find that the evidence maintained by a social media website is “private,” in which case the SCA prohibits a non-governmental entity, such as Facebook and MySpace, from disclosing that information without the consent of the owner of the account.⁵⁶

In one high profile example of the hurdles faced by defendants, on October 19, 2012, the court presiding over the Trayvon Martin murder trial granted the defendant’s motion seeking permission to subpoena Facebook and Twitter for the records of Trayvon Martin’s social media accounts as well as Mr. Martin’s girlfriend’s Twitter account.⁵⁷ Notwithstanding the order, Facebook and Twitter may challenge the subpoenas as Twitter has done in *People v. Harris*.

Despite these challenges, criminal defendants may attempt to use novel methods of obtaining exculpatory social media evidence. For example, a law enforcement officer’s social media account records may be obtained under *Brady v. Maryland* or *Giglio v. United States*.⁵⁸

Moreover, courts may order jurors, witnesses or third parties to produce or manipulate their social media information in unique and unprecedented ways. For example, courts have done the following:

- (1) ordered a juror to “execute a consent form sufficient to satisfy the exception” in the SCA to allow Facebook to produce the juror’s wall posts to defense counsel;⁵⁹
- (2) ordered a party to briefly change his Facebook profile to include a prior photograph so that his

Facebook pages could be printed as they existed at a prior time;⁶⁰

(3) recommended that an individual “friend” the judge on Facebook in order to facilitate an in camera review of Facebook photos and comments;⁶¹ and

(4) ordered parties to exchange social media account user names and passwords.⁶²

Such novel avenues of access to social media evidence may be considered where the defendant subpoenas a social media provider for certain records of a witness or victim and the social media company objects to the subpoena pursuant to the SCA or is unable to produce the evidence as it previously existed.

ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

Social media is subject to the same rules of evidence as paper documents or other electronically stored information, but the unique nature of social media—as well as the ease with which it can be manipulated or falsified⁶³—creates hurdles to admissibility not faced with other evidence.

The challenges surrounding social media evidence demand that one consider admissibility when social media is preserved, collected, and produced.

It is important for counsel to memorialize each step of the collection and production process and to consider how counsel will authenticate a Tweet, Facebook posting, or photograph, for example: by presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it), by searching the computer itself to see if it was used to post or create the information, or by attempting to obtain the information in question from the actual social media company that maintained the information the ordinary course of their business.

Notably, these same challenges face the government who must also consider admissibility of social media when they conduct their investigation. In *United States v. Stirling*, the government seized the defendant’s computer pursuant to a search warrant and provided the defendant with a forensic copy of the hard drive.⁶⁴

The government also performed a forensic examination of the hard drive and extracted 214 pages of Skype chats downloaded from the defendant’s computer—chats that were not “readily available by opening the folders appearing on the hard drive”—but did not provide this information to the defense until the morning of its expert’s testimony near the end of trial.⁶⁵

The logs “had a devastating impact” on the defendant because they contradicted many of his statements made during his testimony, and he was convicted.⁶⁶

In a short but stinging opinion ordering a new trial, the court found:

While both government and defense attorneys grapple with addressing and authenticating social media sources of evidence, courts largely seem to be erring on the side of admissibility and leaving any concerns about the evidence itself—such as who authored the evidence or whether the evidence is legitimate—to jurors to decide what weight that evidence should be given.

For example, social media evidence has been ruled admissible where the content of the evidence contains sufficient indicia that it is the authentic creation of the purported user.⁶⁸ In *Tienda v. State*,⁶⁹ the appellant was convicted of murder based in part on evidence obtained by the prosecutors after subpoenaing MySpace. Specifically, “the State was permitted to admit into evidence the names and account information associated with [the defendant’s MySpace.com profiles], photos posted on the profiles, comments and instant messages linked to the accounts, and two music links posted to the profile pages.”⁷⁰

The Court of Criminal Appeals affirmed the trial judge and concluded that the MySpace profile exhibits used at trial were admissible because they were “sufficient indicia of authenticity” that “the exhibits were what they purported to be—MySpace pages the contents of which the appellant was responsible for.”⁷¹

In another recent case, a defendant was charged with aggravated assault following a domestic dispute with his girlfriend.⁷² At trial, the prosecution introduced Facebook messages sent from the defendant’s account in which he regretted striking his girlfriend and asked for her forgiveness. The defendant denied sending the Facebook messages, and argued that both he and his girlfriend had access to each other’s Facebook accounts.

Acknowledging that electronic communications are “susceptible to fabrication and manipulation”, the court allowed the messages to be authenticated through circumstantial evidence, most notably that they were sent from the defendant’s account and that the girlfriend testified that she did not send the messages.⁷³

In another instance, a federal court held that photographs of a defendant from his MySpace page, which depicted him holding cash, were relevant in his criminal trial for possession of firearms and drugs but withheld ruling on the admissibility of the photos and whether they presented a risk of unfair prejudice.⁷⁴

Given the proliferation of social media, the increasing sophistication of technology, and the potential challenges relating to the reliability or authentication of social media, the authentication and admissibility of such evidence will likely be the subject of vigorous disputes between parties that may mean the difference between ultimate guilt and innocence.

CONCLUSION

Social media evidence is undeniably a critical, new frontier of government investigations and criminal proceedings. Social media has rapidly become so pervasive that while users are creating warehouses of data every day and while social media companies roll out new communication features, courts, government agencies, practitioners and the social media companies themselves are struggling to understand how this information fits into existing legal paradigms of constitutional protections, the SCA and rules of evidence.

Despite this uncertainty, one thing is clear—the government has a deep and largely one-sided set of tools for seeking out and obtaining social media evidence that plays an ever-increasing critical role in their investigations and litigation.

Justin P. Murphy is a counsel in Crowell & Moring's Washington, D.C. office where he practices in the firm's White Collar & Regulatory Enforcement Group and E-Discovery and Information Management Group. Adrian Fontecilla is an associate in Crowell & Moring's Washington, D.C. office where he practices in the firm's Antitrust Group.

© 2013 Bloomberg Finance L.P. All rights reserved. Bloomberg Law Reports ® is a registered trademark and service mark of Bloomberg Finance L.P.

Disclaimer

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.