Bloomberg BNA

Digital Discovery & e-Evidence®

BNA INSIGHT

This article examines the importance of social media in government investigations and criminal litigation, including accessing and utilizing social media evidence, constitutional issues raised by social media evidence, and the authentication and admissibility of such evidence.

Social Media Evidence in Criminal Proceedings: An Uncertain Frontier

By Justin P. Murphy and Adrian Fontecilla

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.

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.

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

[1] Experian Marketing Services, *The 2012 Digital Marketer: Benchmark and Trend Report*, at 79, http://www.experian.com/simmons-research/register-2012-digital-marketer.html (last visited Oct. 24 2012).

[2] Netpop Research, *Connect: Social Media Madness U.S. 2012* (April 2012), http://www.netpopresearch.com/social-media-madness.

[3] Tom Webster, *The Social Habit 2011* (May 29, 2011), http://www.edisonresearch.com/home/archives/2011/05/the_social_habit_2011.php.

[4] Mark Zuckerberg, *One Billion People on Facebook* (Oct. 4, 2012), http://newsroom.fb.com/News/One-Billion-People-on-Facebook-1c9.aspx.

[5] *Twitter Turns Six* (Mar. 21, 2012), http://blog.twitter.com/2012/03/twitter-turns-six.html.

 ISSN 1941-3882

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:

> [W]here 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. While [defendant] undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his 'friends' would keep his profile private. And the wider his circle of 'friends', the more likely [defendant's] posts would be viewed by someone he never expected to *see* them. [Defendant's] legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted — including sharing it with the Government.[16]

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

---

[6] Josh James, *How Much Data is Created Every Minute?* (June 8, 2012), http://www.domo.com/blog/2012/06/how-much-data-is-created-every-minute/.

[7] Pingdom, *Report: Social Network Demographics in 2012* (Aug. 21, 2012), http://royal.pingdom.com/2012/08/21/report-social-network-demographics-in-2012/.

[8] *See Quagliarello v. Dewees*, No. 09-4870, 2011 BL 203183, at *2 (E.D. Pa. Aug. 4, 2011) (''As the use of social media such as MySpace and Facebook has proliferated, so too has the value of these websites as a source of evidence for litigants.'').

[9] Earlier this year, the Boston Police Department publicly released the case files of the alleged ''Craigslist Killer,'' Philip Markoff, who committed suicide while awaiting trial. Those case files include the District Attorney's subpoena to Facebook as well as Facebook's response. Carly Carioli, *When The Cops Subpoena Your Facebook Information, Here's What Facebook Sends the Cops* (Apr. 6, 2012), http://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx.

[10] Electronic Frontier Foundation, *2012: When the Government Comes Knocking, Who Has Your Back?* (May 31, 2012), https://www.eff.org/sites/default/files/who-has-your-back-2012_0_0.pdf.

[11] *See, e.g.*, *United States v. Anderson*, 664 F.3d 758, (8th Cir. 2012) (defendant sentenced to 12 years in prison based in part on over 800 private chats with adolescent girls that were obtained through a search warrant for defendant's Facebook account).

[12] *See, e.g.*, U.S. Dep't of Homeland Security, *Publicly Available Social Media Monitoring and Situational Awareness Initiative* (June 22, 2010); *see also* LexisNexis, *Role of Social Media in Law Enforcement Significant and Growing* (July 18, 2012), http://www.lexisnexis.com/media/press-release.aspx?id=1342623085481181 (over 80 percent of local and federal agencies use social media during investigations).

[13] Saba, *New Study Shows 66 percent of Government Organizations Have Adopted Social Networking, Collaboration Tools* (Jan. 14, 2010), http://www.saba.com/company/press-releases/2010/saba-and-hci-publish-study-of-social-networking-in-government/.

[14] *See, e.g.*, *United States v. Robison*, No. 11CR380 DWF/TNL, 2012 BL 332169, at *16 (D. Minn. Mar. 16, 2012) (law enforcement created fake online identity and became Facebook friends with defendant, ''which permitted [the government] to view [defendant's] name and photo on his Facebook account''); *United States v. Phillips*, Criminal No. 3:06–CR–47, 2009 BL 294552 (N.D. W.Va. July 1, 2009) (government ''created an undercover user profile on www.myspace.com'').

[15] *United States v. Meregildo*, No. 1:11-cr-00576-WHP, 2012 BL 211810 (S.D.N.Y. Aug. 10, 2012).

[16] *Id.* at *2.

  DDEE ISSN 1941-3882

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 funda-

---

[17] *Twitter Transparency Report* (July 2, 2012), http://blog.twitter.com/2012/07/twitter-transparency-report.html.

[18] *Id.*

[19] *FAQ–Google Transparency Report*, http://www.google.com/transparencyreport/userdatarequests/faq/ (last visited Oct. 24, 2012).

[20] *Visible Changes – Google Transparency Report,* http://www.google.com/transparencyreport/userdatarequests/data/ (last visited Oct. 24, 2012).

[21] LexisNexis, *supra* note 13.

[22] *See, e.g.*, *Anderson*, 664 F.3d at 762 (hundreds of Facebook private chats obtained through a search warrant); *Meregildo*, 2012 BL 211810, at *2 (evidence obtained through warrant issued to Facebook); *People v. Harris*, 949 N.Y.S.2d 590, 597 (N.Y. Crim. Ct. 2012) (state sent Twitter a subpoena seeking to obtain defendant's user information and Tweets); *United States v. Sayer*, 2:11-CR-113-DBH, 2012 BL 145681, at *3 (D. Me. June 13, 2012) (subpoenas used to obtain evidence from Facebook and MySpace); *In re Grand Jury Subpoena No. 11116275*, 846 F. Supp. 2d 1, 2 (D.D.C. 2012) (denying anonymous intervenor's motion to quash a subpoena issued to Twitter by a federal grand jury for records pertaining to the intervenor's identity); *United States v. Kearney*, 672 F.3d 81, 84-85 (1st Cir. 2012) (law enforcement used account and IP address information obtained from MySpace via an administrative subpoena to subpoena defendant's internet provider for his name and address).

[23] *See United States v. Warshak*, 631 F.3d 266, 282 (6th Cir. 2010) (citing 18 U.S.C. §§ 2701 et seq.); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010) (applying the SCA to subpoenas issued to Facebook and MySpace while recognizing that no courts ''have addressed whether social networking sites fall within the ambit of the statute'').

[24] *See* Rudolph J. Burshnic, Note, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259, 1264 (2012).

[25] *See, e.g.*, *Hubbard v. MySpace, Inc.*, 788 F. Supp. 2d 319 (S.D.N.Y. 2011) (search warrant served by state authorities on MySpace to produce, among other things, the account IP address, the contents of the account user's inbox, and sent email was sufficient to satisfy the requirements of the Stored Communications Act); *Crispin*, 717 F. Supp. 2d at 991 (acknowledging the privacy settings of the user, the court quashed subpoenas seeking private messages on Facebook and MySpace as they were protected under the Stored Communications Act).

[26] 18 U.S.C. § 2703(c)(2); *id.* § 2703(d).

[27] *Warshak*, 631 F.3d at 282-83 (citation omitted).

[28] *Id.*

[29] *Id.* at 288.

[30] *Id.* (citations omitted).

mental 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]

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

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]

[31] *Id.* at 285-286.

[32] *See id.* at 288 (warrantless seizure of emails from ISP pursuant to SLA violated Fourth Amendment); Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 Marq. L. Rev. 1495, 1513-33 (2010) (arguing that individuals should have Fourth Amendments rights in their privately shared information on social networking platforms).

[33] As of the date of this article's publication, a decision had not yet been issued by the appellate court.

[34] Brief for Non-Party Movant-Appellant, *People v. Harris*, No. 2011 080152 (N.Y. App. Div. 1st Dep't Aug. 27, 2012).

[35] *Harris*, 949 N.Y.S.2d at 597.

[36] Twitter, *Guidelines for Law Enforcement*, http://support.twitter.com/entries/41949-guidelines-for-law-enforcement#section9 (last visited Oct. 24, 2012).

[37] Electronic Frontier Foundation, *supra* note 11.

[38] Somini Sengupta, *Twitter's Free Speech Defender*, N.Y. Times, Sept. 2, 2012.

[39] Brief for Non-Party Movant-Appellant, *People v. Harris*, at *13.

[40] *Id.* at *18-19.

[41] *Id.* at *18 (citing *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010)).

[42] *Id.* at *21.

[43] *Id.* at *22 (citing *United States v. Jones*, 132 S. Ct. 945, 949 (2012)).

[44] Doug Austin, *Twitter Turns Over Tweets in People v. Harris* (Oct. 3, 2012), http://www.ediscoverydaily.com/2012/10/twitter-turns-over-tweets-in-people-v-harris-ediscovery-case-law.html.

[45] *Meregildo*, 2012 BL 211810, at *2.

[46] *R.S. v. Minnewaska Area Sch. Dist. No. 2149*, No. 12-cv-00588-MJD-LIB, 2012 BL 227182, at *12 (D. Minn. Sept. 6, 2012) (finding that sixth grader had reasonable expectation of privacy in private messages exchanged via her password-protected Facebook account); *see also Crispin*, 717 F. Supp. 2d at 991.

[47] *See* Facebook, *How Can I Control What Stories Display on My Wall?*, http://www.facebook.com/help/facebook-

  DDEE ISSN 1941-3882

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]

[C]riminal defendants may attempt to use novel methods of obtaining exculpatory social media evidence.

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

questions#!/help/218066191556033/ (last visited Oct. 24, 2012).

[48] *See In re Target Email Address*, No. 12-MJ-08119-DJW, 2012 BL 258633 (D. Kan. Sept. 21, 2012) (holding that an individual has a Fourth Amendment right of privacy to emails and online faxes stored with, sent to, or received through third-party internet service providers).

[49] *See Warshak*, 631 F.3d at 284-85 (''[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.'').

[50] Daniel K. Gelb, *Defending a Criminal Case from the Ground to the Cloud*, 27-SUM Crim. Just. 28 (2012).

[51] *See* Zach Winnick, *Social Media an Ethical Minefield for Attorneys*, Law360, Apr. 13, 2012, http://www.law360.com/articles/329795/social-media-an-ethical-minefield-for-attorneys (describing ethical concerns regarding private counsel's use of social networking sites in connection with litigation that are generally not shared by government authorities in investigations).

[52] *See, e.g.*, Philadelphia Bar Ass'n , Prof. Guidance Comm., *Opinion 2009-02* (March 2009) (concluding that a social media friend request to a witness in the litigation for the purpose of gathering social media evidence is ''deceptive'' and in violation of ethical rules); N.Y. State Bar Ass'n, Committee on Prof'l Ethics, *Opinion 843 (9/10/10)* (Sept. 10, 2010) (accessing publicly available social media evidence is permissible but 'friending'' another party to do so is not); San Diego County Bar Legal Ethics Committee, *SDCBA Legal Ethics Opinion 2011-02* (May 24, 2011) (ethics rules bar attorneys from making ex parte friend request of a represented party or 'deceptive' friend requests of unrepresented witnesses).

[53] In criminal litigation, the majority of evidence, electronic or otherwise, is collected by the government prior to indictment and Federal Rule of Criminal Procedure 16 does not require the government to produce such evidence unless it is being used in their case-in-chief.

[54] *Id.*

[55] Fed. R. Crim. P. 17(e)(1).

[56] 18 U.S.C. § 2703.

[57] Erin Fuchs, *A Jury Will Likely Scrutinize Trayvon Martin's Deleted Facebook and Twitter Accounts* (Oct.19, 2012), http://www.businessinsider.com/zimmerman-can-subpoena-social-media-2012-10.

[58] *See Brady v. Maryland*, 373 U.S. 83 (1963); *Giglio v. United States*, 405 U.S. 150 (1972).

[59] *Juror Number One v. California*, No. CIV. 2:11-397 WBS JFM, 2011 BL 38413, at *1 (E.D. Cal. Feb. 14, 2011).

[60] *Katiroll Co. v. Kati Roll and Platters, Inc.*, No. 10-3620 (GEB), 2011 BL 200991, at *4 (D.N.J. Aug. 3, 2011).

[61] *Barnes v. CUS Nashville, LLC*, No. 3:09-CV-00764, 2010 BL 125058, at *1 (M.D. Tenn. June 3, 2010).

(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 falsified[63]—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:

> [If a defendant] needs to hire a computer forensics expert and obtain a program to retrieve information not apparent by reading what appears in a disk or hard drive, then such a defendant should so be informed by the Government, which knows of the existence of the non-apparent information. In such instance, and without the information or advice to search metadata or apply additional programs to the disk or hard drive, production has not been made in a reasonably usable form. Rather, it has been made in a manner that disguises what is available, and what the Government knows it has in its arsenal of evidence that it intends to use at trial.[67]

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]

[S]ocial 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.

In another recent case, a defendant was charged with aggravated assault following a domestic dispute with

[62] *See, e.g.*, *Gallion v. Gallion*, No. KNO-FA-11-4116955-S, at *1 (Conn. Super. Ct. Sept. 30, 2011) (ordering parties to exchange passwords to Facebook and a dating website); *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 BL 318557, at *5 (Pa. Com. Pl. Sept. 9, 2010) (ordering plaintiff to produce Facebook and MySpace login credentials to opposing counsel for ''read-only access'').

[63] *See, e.g.*, *Griffin v. State*, 19 A.3d 415, 424 (Md. 2011) (collecting cases similarly recognizing ''[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator'').

[64] Order on Defendant's Motion for New Trial, *United States v. Stirling*, No. 1:11-cr-20792-CMA, slip op. at 2 (S.D. Fla. June 5, 2012).

[65] *Id.* at 2.

[66] *Id.*

[67] *Id.* at 4-5.

[68] *See, e.g.*, *People v. Lesser*, No. H034189 (Cal. Ct. App. Jan. 21, 2011) (officer's testimony that he cut and pasted portions of internet chat transcript was sufficient for admissibility); *People v. Valdez*, No. G041904, 135 Cal. Rptr. 3d 628, 633 (Cal. Ct. App. 2011) (conviction upheld where the court correctly admitted a trial exhibit consisting of printouts of defendant's MySpace page, which the prosecution's gang expert relied on in forming his opinion that defendant was an active gang member); *People v. Fielding*, No. C06022 (Cal. Ct. App. June 18, 2010) (incriminating MySpace messages sent by defendant authenticated by victim who testified he believed defendant had sent them; inconsistencies and conflicting inferences regarding authenticity goes to weight of evidence, not its authenticity).

[69] *Tienda v.* State, 358 S.W.3d 633, 634-35 (Tex. Crim. App. 2012).

[70] *Id.* at 635.

[71] *Id.* at 647.

  DDEE ISSN 1941-3882

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]

[72] *Campbell v. Texas*, No. 03-11-00834-CR, 2012 BL 225712, at *2 (Tex. App. Aug. 31, 2012).

[73] *Id.* at *4.

[74] *United States v. Drummond*, No. 1:09-cr-00159, 2010 BL 68549, at *2 (M.D. Pa. March 29, 2010). The defendant ultimately entered a guilty plea and there was no final ruling by the court on the admissibility of the photographs.

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.