Richmond Journal of Law and Technology

Volume 19 | Issue 3 Article 4

2013

Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues

Justin P. Murphy

Adrian Fontecilla

Richmond Journal of Law & Technology Volume XIX, Issue 3

SOCIAL MEDIA EVIDENCE IN GOVERNMENT INVESTIGATIONS AND CRIMINAL PROCEEDINGS: A FRONTIER OF NEW LEGAL ISSUES

By Justin P. Murphy and Adrian Fontecilla*

Cite as: Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH 11 (2013), *available at* http://jolt.richmond.edu/v19i3/article11.pdf.

I. INTRODUCTION

[1] As the newest pillar of communication in today's society, social media is revolutionizing how the world does business, discovers and shares news, and instantly engages with friends and family. Not surprisingly, because social media factors into the majority of cases in some respect, this exploding medium significantly affects government investigations and criminal litigation. Social media evidence includes, among other things, photographs, status updates, a person's location at a certain time, and direct communications to or from a defendant's social media account. This Article will examine the importance of social media in government investigations and criminal litigation, including access to and use of social media evidence, constitutional issues that social media evidence raises, the authentication and admissibility of such evidence, in addition to the impact of social media on jurors.

II. THE IMPORTANCE OF SOCIAL MEDIA

[2] Social media use is widespread. Ninety-one percent of today's online adults use social media regularly, which has become the number

one activity on the web.[1] "People continue to spend more time on social networks than any other category of [web]sites," accounting for "20% of their time spent on PCs and 30% of their mobile [use] time."[2] Social media use in the United States alone has increased by 356% since 2006.[3] 52% of Americans now have at least one social media profile,[4] more than one billion people use Facebook actively each month,[5] and 32% of all Internet users are now using Twitter.[6] Notably, some of the largest growth in the last year has been among forty-five to fifty-four year old Americans,

* 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. Both are contributors to Crowell & Moring's E-Discovery Law Insights blog - http://www.ediscoverylawinsights.com/.

[1] EXPERIAN MARKETING SERVICES, THE 2012 DIGITAL MARKETER: BENCHMARK AND TREND REPORT 79 (2012), *available at* http://www.experian.com/simmons-research/register-2012-digital-marketer.html.

[2] NIELSEN, STATE OF THE MEDIA: SOCIAL MEDIA REPORT 2012, at 4 (2012), *available at* http://blog.nielsen.com/nielsenwire/social/2012/ (last visited Dec. 31, 2012).

[3] *Connect: Social Media Madness U.S. 2012*, NETPOP RESEARCH (April 2012), *available at* http://netpopresearch.com/social-media-madness.

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

[5] Aaron Smith, Laurie Segall & Stacy Cowley, *Facebook Reaches One Billion Users*, CNN MONEY (Oct. 4, 2012, 9:50 AM), http://money.cnn.com/2012/10/04/technology/facebook-billion-users/index.html.

[6] Brian Honigman, *100 Fascinating Social Media Statistics and Figures From 2012*, HUFFINGTON POST (Nov. 11, 2012, 7:32 PM), http://www.huffingtonpost.com/brian-honigman/100-fascinating-social-me_b_2185281.html.

55% of whom now have a profile on a social networking site.[7]

[3] There are hundreds of social networking websites with each catering to a different demographic and providing a different type of content.[8] Moreover, their users are constantly creating massive amounts of data. "Twitter users send [one] billion tweets every two and a half days,"[9] Instagram users upload forty million images every day,[10] Facebook users share 684,478 pieces of content every minute, and YouTube users upload forty-eight hours of new video every minute.[11] Social media users create more than just photos, videos, and tweets. They share other information, such as their location as well. "As of 2012, [seventeen] billion location-tagged posts and check-ins were logged."[12] The myriad and continually changing ways to share information via social media has resulted in a digital goldmine of potential evidence, such as profiles, lists of friends, group memberships, messages, chat logs, tweets, photos, videos, tags, GPS locations, likes, check-ins, and login

[7] Erik Qualman, *10 New 2012 Social Media Stats = WOW!*, SOCIALNOMICS, http://www.socialnomics.net/2012/06/06/10-new-2012-social-media-stats-wow/ (last visited Dec. 31, 2012).

[8] *See* PINGDOM, SOCIAL NETWORK DEMOGRAPHICS IN 2012 (2012), *available at* http://royal.pingdom.com/2012/08/21/report-social-network-demographics-in-2012/.

[9] *Nielsen and Twitter Establish Social TV Rating*, NIELSEN (Dec. 17, 2012), http://www.nielsen.com/us/en/insights/press-room/2012/nielsen-and-twitter-establish-social-tv-rating.html.

[10] *Instagram Press Center*, INSTAGRAM, http://instagram.com/press/ (last visited Feb. 1, 2013).

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

[12] Honigman, *supra* note 6.

timetables.[13]

[4] The information that social media providers make available 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 like Facebook responds to a government subpoena, it could provide the user's profile, wall posts, photos that the user uploaded, 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.[14] In addition, with the advent of location-based services that social media companies like Facebook, Twitter, and FourSquare offer, precise location information will be increasingly maintained in the ordinary course of business and subject to the same subpoenas and search warrants.[15] One newsworthy example demonstrating the amount of information available to law enforcement from a simple photograph is that of John McAfee, the antivirus company founder who was recently on the run from law enforcement authorities investigating the murder of his neighbor. McAfee was forced out of hiding when it was found that a

[13] *See* Quagliarello v. Dewees, No. 09-4870, 2011 WL 3438090, 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.").

[14] *See, e.g.*, Carly Carioli, *When the Cops Subpoena Your Facebook Information, Here's What Facebook Sends the Cops*, THE PHOENIX (Apr. 6, 2012, 8:30 AM), http://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx (noting the breadth of information Facebook provided in response to a subpoena from the Boston Police Department).

[15] *Cf.* MARCIA HOFMANN ET AL., ELEC. FRONTIER FOUND., 2012: WHEN THE GOVERNMENT COMES KNOCKING, WHO HAS YOUR BACK? 7 (2012), *available at* https://www.eff.org/sites/default/files/who-has-your-back-2012_0_0.pdf (discussing issues arising from government access to location data and the companies that collect data).

photo of him published on a blog was embedded with GPS metadata pinpointing his exact location in Guatemala.[16] Not surprisingly, each social media request can yield admissions or incriminating photos in addition to other evidence.[17]

III. ACCESSING PUBLICLY AVAILABLE SOCIAL MEDIA EVIDENCE

[5] It is no secret that government agencies mine social networking websites for evidence. Even without having to seek a warrant from the court or issue a subpoena, there are troves of social media evidence publicly available.[18] For example, the New York Police Department has a social media unit that mines Facebook, Twitter, and other social media sites for evidence of crimes and potential criminal activity.[19] Moreover, a

[16] Eyder Peralta, *Betrayed By Metadata: John McAfee Admits He's Really in Guatemala*, NPR (Dec. 4, 2012, 12:24 PM), http://www.npr.org/blogs/thetwo-way/2012/12/04/166487197/betrayed-by-metadata-john-mcafee-admits-hes-really-in-guatemala.

[17] *See, e.g.*, United States v. Anderson, 664 F.3d 758, 761-62 (8th Cir. 2012) (affirming the conviction of a defendant sentenced to 12 years in prison based in part on over 800 private chats with adolescent girls and inappropriate pictures that were obtained through a search warrant for defendant's Facebook account).

[18] *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE OFFICE OF OPERATIONS COORDINATION AND PLANNING: PUBLICLY AVAILABLE SOCIAL MEDIA MONITORING AND SITUATIONAL AWARENESS INITIATIVE 3 (2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia.pdf (noting that the National Operations Center will use publicly available search engines and content aggregators to monitor activities on social media sites); *see also Role of Social Media in Law Enforcement Significant and Growing*, LEXISNEXIS (July 18, 2012), http://www.lexisnexis.com/media/press-release.aspx?id=1342623085481181 (stating that, according to the results of a comprehensive survey, over eighty percent of local and federal agencies use social media during investigations).

[19] Rocco Parascandola, *NYPD Forms New Social Media Unit to Mine Facebook and Twitter for Mayhem*, NY DAILY NEWS (Aug. 10, 2011, 4:00 AM),

majority of government agencies are active participants who contribute content and solicit information through social media.[20] Given the amount of information publicly available and the avenues that the government has to seek out such information, usually the government does not need a search warrant, subpoena, or court order to obtain social media evidence.

[6] There are countless cases involving defendants who are arrested because of information, photos, or admissions posted to social media sites. For example, a defendant in Kentucky was jailed after he posted a photo of himself siphoning gas from a police car onto Facebook.[21] Another defendant broke into a Washington, D.C. home to steal a coat, a laptop, and cash, subsequently using the victim's laptop to post a picture of himself wearing the stolen coat and holding up the stolen cash to the victim's Facebook page.[22] The photo was used later to secure a guilty plea from the defendant.[23] While some sites allow users to control what content the public can access, many users do not make use of such tools. In fact, twenty five percent of Facebook users do not use any type of

http://www.nydailynews.com/new-york/nypd-forms-new-social-media-unit-facebook-twitter-mayhem-article-1.945242.

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

[21] *See generally* Eric Larson, *8 Dumb Criminals Caught Through Facebook*, MASHABLE (Dec. 12, 2012), http://mashable.com/2012/12/12/crime-social-media/.

[22] *Id.*

[23] *Id.*

privacy controls.[24]

[7] In addition to searching for publicly available evidence, government agents are allowed to go further than defense counsel 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.[25] For example, in *United States v. Meregildo*, the defendant adjusted the privacy settings on his Facebook account so that only his Facebook "friends" could view his postings.[26] The government obtained the incriminating evidence against the defendant through a cooperating witness who happened to be Facebook "friends" with the defendant.[27] The defendant moved to suppress the evidence seized from his Facebook account, arguing that the government had violated his Fourth Amendment rights.[28] The court found:

[24] *See* Shea Bennett, *Facebook, Twitter, Pinterest, Instagram – Social Media Statistics and Facts 2012*, ALL TWITTER (Nov. 1, 2012, 6:00 AM), http://www.mediabistro.com/alltwitter/social-media-stats-2012_b30651.

[25] *See, e.g.*, United States v. Robison, No. 11CR380 DWF/TNL, 2012 WL 1110086, at *1-2 (D. Minn. Mar. 16, 2012) (noting that law enforcement created fake online identity and became Facebook friends with defendant, "which permitted [the government] to view [the defendant's] name and photo on his Facebook account"); United States v. Phillips, Criminal No. 3:06–CR–47, 2009 WL 1918931, at *7 (N.D. W. Va. July 1, 2009) (noting that the government "created an undercover user profile on www.myspace.com").

[26] United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012).

[27] *Id.*

[28] *Id.* at *1.

> 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. . . . While [the 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 [the defendant's] posts would be viewed by someone he never expected to see them. [The 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.[29]

[8] Recently, federal authorities relied heavily on social media to build their case against four defendants who were allegedly involved in an Al Qaeda inspired terrorist cell based in California.[30] The criminal complaint, which included a section titled "Defendants' Social Media," provides a glimpse into the various ways that law enforcement uses social media in its investigations.[31] The investigators used an "online covert employee" who posed as a terrorism sympathizer to elicit damaging statements from the defendants, recorded Skype conversations between a confidential informant and the defendants, and relied on the social media

[29] *Id.* at *2 (internal citations omitted).

[30] Ryan Gallagher, *Feds Monitor Facebook "Likes," Infiltrate Skype Chats To Build Terrorism Case*, SLATE (Nov. 29, 2012, 4:33 PM), http://mobile.slate.com/blogs/future_tense/2012/11/29/facebook_likes_skype_used_to_build_fbi_case_against_california_terrorism.html.

[31] Complaint at ¶¶ 26-28, United States v. Kabir, No. ED12-0431M (C.D. Cal. Nov. 16, 2012), 2012 WL 6576560.

content that each defendant "liked," "shared," or on which the defendant commented.[32]

[9] The Securities and Exchange Commission also recently issued a Wells Notice for the first time based on a social media communication.[33] On December 5, 2012, Netflix disclosed that it had received a Wells Notice from the SEC Enforcement Staff for allegedly violating public disclosure rules when its CEO, Reed Hastings, posted onto his Facebook with more than 200,000 followers that, "Netflix monthly viewing exceeded one billion hours for the first time ever in June [2012]."[34] After receiving the notice, Hastings noted in a letter to shareholders that, "[W]e think posting to over 200,000 people is very public, especially because many of my subscribers are reporters and bloggers;" nevertheless, the SEC has provided no formal guidance concerning the use of social media, Regulation FD, and communications with the investing public. [35]

IV. SOCIAL MEDIA COMPANIES, SUBPOENAS, AND WARRANTS

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

---

[32] Gallagher, *supra* note 30.

[33] *See* Netflix Form 8-K filed Dec. 5, 2012; CHRISTOPHER GARCIA & MELANIE CONROY, REG FD ALERT: APPLYING SECURITIES LAWS TO SOCIAL MEDIA COMMUNICATIONS 1 (2012), *available at* http://www.weil.com/files/upload/Weil_Alert_Sec_Lit_Enforcement_Dec_21_2012.pdf.

[34] *Id.* at 2.

[35] *See Netflix CEO's Facebook Post Triggered SEC Wells Notice*, CNBC (Dec. 7, 2012, 7:10 AM), http://www.cnbc.com/id/100289227/Netflix_CEO039s_Facebook_Post_Triggered_SEC_Wells_Notice; GARCIA & CONROY, *supra* note 33, at 1.

For example, Twitter "received more government requests" for user information in the "first half of 2012 . . . than in the entirety of 2011."[36] In addition, approximately 80% of those requests were from authorities in the United States.[37] Google, which operates social networking sites including YouTube and Google+, continues to receive subpoenas and search warrants in criminal matters at a rapidly accelerating pace. Statistics published by Google, which "primarily cover requests in criminal matters,"[38] show that the number of Google user data requests received from government authorities in the United States more than doubled from 2009 to 2012 and that the United States accounts for over 39% of user data requests received from government authorities around the world.[39]

[11] 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 reveals that social media is widely used to

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

[37] *Id.*

[38] *Transparency Report—FAQ*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/faq/ (last visited Jan.15, 2013).

[39] *Transparency Report—User Data Requests,* GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US/ (last visited Jan. 16, 2013) (demonstrating that requests increased from 3,580 in a period between July to December 2009 to 8,438 in a period from July to December 2012); *Transparency Report—User Data Requests,* GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?t=table (last visited Feb. 8, 2013) (demonstrating that the United States accounts for 8,438 of the 21, 389 user data requests Google received from July to December 2012).

assist in investigations, few learned how to use social media for investigations through formal training, and "74% of those not currently using it . . . intend to start using it."[40] Moreover, the case law is already replete with instances in which the government obtained social media evidence through a warrant or subpoena directed at a social media company.[41] 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 that social media companies maintain.

V. ACCOUNTING FOR THE STORED COMMUNICATIONS ACT

[12] 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

[40] *Role of Social Media in Law Enforcement Significant and Growing*, *supra* note 18.

[41] *See, e.g.*, United States v. Anderson, 664 F.3d 758, 762 (8th Cir. 2012) (noting hundreds of Facebook private chats obtained through a search warrant); United States v. Kearney, 672 F.3d 81, 84 (1st Cir. 2012) (noting that 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); *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. Sayer, Criminal No. 2:11 cr 113 DBH, 2012 WL 2180577, at *3 (D. Me. June 13, 2012) (using subpoenas to obtain evidence from Facebook and MySpace); United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012) (obtaining evidence through warrant issued to Facebook); People v. Harris, 949 N.Y.S.2d 590, 597 (N.Y. Crim. Ct. 2012) (observing that state sent Twitter a subpoena seeking to obtain defendant's user information and Tweets).

circumstances.[42] Passed in 1986, the SCA 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.[43] Consequently, courts will continue to play a critical role in defining how and whether the SCA applies to the varying features of different social media services by applying precedent from older technologies, such as text messaging pager services or electronic bulletin boards.[44]

[13] The SCA provides that non-content records can be compelled through a warrant or court order.[45] With regard to the compelled disclosure of communication content, the SCA provides different levels of statutory privacy protection depending on how long the content has been in electronic storage.[46] The government may obtain content that has been in electronic storage for 180 days or less "only pursuant to a warrant."[47]

---

[42] *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (citing 18 U.S.C. §§ 2701-2711); *see also* 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").

[43] *See* Rudolph J. Burshnic, Note, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1261-64 (2012).

[44] *See, e.g.*, Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319, 321-27 (S.D.N.Y. 2011) (holding that 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).

[45] *See* 18 U.S.C. § 2703(c)(1)(a)-(b) (2006).

[46] *See Warshak,* 631 F.3d at 283.

[47] *Id.*

"The government has three options for obtaining communications . . . that have been in electronic storage with an electronic 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)."[48]

[14] At least one Circuit Court of Appeals has called into question the constitutionality of the SCA.[49] 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] e-mails" without a warrant and added that, "to the extent that the SCA purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional."[50] The court reasoned that "[o]ver the last decade, e-mail 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, "e-mail requires strong protection under the Fourth Amendment."[51] Noting that e-mail was analogous to a phone call or letter and that the internet service provider was the intermediary who made e-mail communication possible, the functional equivalent of a post office or telephone company, the court concluded that given "the fundamental similarities between e-mail and traditional forms

[48] *Id.* (citation omitted). Since *Warshak*, most major providers state that they require a search warrant to compel the stored contents of any account. *See, e.g.*, *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ (last visited Jan. 2, 2012) ("A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.").

[49] *See Warshak*, 631 F.3d at 288.

[50] *Id*.

[51] *Id.* at 286 (citations omitted).

of communication, it would defy common sense to afford e-mails lesser Fourth Amendment protection."[52] However, Congress made clear that changing the law will require extended consideration when, on December 24, 2012, the Senate removed from proposed legislation an amendment to the SCA that would have prevented authorities from viewing a person's e-mail messages without obtaining a warrant.[53] In the meantime, courts will play a key role in clarifying how the SCA applies not only to e-mails, but also to the social media that has rapidly become as pervasive and important to people as e-mail.

VI. DEFINING A DEFENDANT'S CONSTITUTIONAL RIGHTS REGARDING SOCIAL MEDIA EVIDENCE

[15] Courts have also started grappling with novel issues relating to the constitutionality of the government's use of information obtained from social media companies in criminal proceedings.[54] For example, a New York appellate court will soon issue an opinion regarding Twitter's appeal of two court orders in the prosecution of an Occupy Wall Street protestor in *People v. Harris*.[55] The trial court held that the defendant lacked standing to move to quash the government's third-party subpoena to

[52] *Id.* at 285-86.

[53] *See* Noel Brinkerhoff, *Congress, at Last Minute, Drops Requirement to Obtain Warrant to Monitor Email*, ALLGOV (Dec. 25, 2012), http://www.allgov.com/news/top-stories/congress-at-last-minute-drops-requirement-to-obtain-warrant-to-monitor-email-121225?news=846578.

[54] *See Warshak*, 631 F.3d at 288 (holding that warrantless seizure of emails from ISP pursuant to SCA violated Fourth Amendment); *see also* Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1513-32 (2010) (arguing that individuals should have Fourth Amendments rights in their privately shared information on social networking platforms).

[55] As of the date of publication, the appeal had not been decided.

Twitter for his account records and that the Fourth Amendment did not protect his tweets.[56] The trial court similarly denied Twitter's motion to quash the government's subpoenas for the defendant's Twitter records for the same reasons.[57] Although Twitter's appeal is pending, Twitter turned over the data after the trial judge threatened the company with civil contempt and fines, which led to the defendant's guilty plea in December 2012.[58]

[16] 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,"[59] a policy which is becoming more common among social media companies.[60] Not only does Twitter notify its users that the company has received a government-issued information request for the user's data, but it also protects its business by litigating

[56] People v. Harris, 945 N.Y.S.2d 505, 510 (N.Y. Crim. Ct. 2012).

[57] *See* People v. Harris, 949 N.Y.S.2d 590, 598 (N.Y. Crim. Ct. 2012) (granting in part and denying in part the motion to quash). The court found in favor of the government for all non-content information and content information from September 15, 2011, to December 30, 2011. Content information less than 180 days old (tweeted on December 31, 2011) could only be disclosed pursuant to a search warrant.

[58] *See* Russ Buettner, *A Brooklyn Protester Pleads Guilty After His Twitter Posts Sink His Case*, N.Y. TIMES, Dec. 12, 2012, at A31, *available at* http://www.nytimes.com/2012/12/13/nyregion/malcolm-harris-pleads-guilty-over-2011-march.html.

[59] *Guidelines for Law Enforcement*, TWITTER, http://support.twitter.com/entries/41949-guidelines-for-law-enforcement#section9 (last visited Jan, 15, 2013).

[60] *See* HOFMANN ET AL, *supra* note 15, at 8-9 ("Dropbox, LinkedIn, Sonic.net and SpiderOak have now joined Twitter in promising to notify their users when possible about government attempts to seek information about them.").

against such third-party government subpoenas.[61]

[17] On appeal, Twitter argued 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.[62] Moreover, Twitter claimed that the Fourth Amendment protects the defendant's tweets, primarily because the government concedes that the defendant did not make public the tweets that it sought.[63] If a defendant has a reasonable expectation of privacy under the Fourth Amendment in his or her non-public e-mails,[64] refusing to afford that same protection to users' non-public tweets would create "arbitrary line drawing."[65] Finally, even assuming that the tweets in question were public, Twitter argued that the government still requires a search warrant under the federal and New York constitutions.[66] Notwithstanding Twitter's pending appeal, Twitter complied with a court order requiring it to promptly submit the

[61] *See* Somini Sengupta, *Twitter's Free Speech Defender*, N.Y. TIMES, Sept. 3, 2012, at B1, *available at* http://www.nytimes.com/2012/09/03/technology/twitter-chief-lawyer-alexander-macgillivray-defender-free-speech.html?pagewanted=all&_r=0.

[62] Brief for Non-Party Movant-Appellant at *12-14, People v. Harris, No. 2011-080152, 2012 WL 3867233 (N.Y. App. Div. Aug. 27, 2012) (noting Twitter's Terms of Service state, "You retain your rights to any Content you submit, post or display on or through the Services" (internal citation omitted)).

[63] *See id*. at *16, 19.

[64] *See id.* at *18-19 (citing United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010)).

[65] *See id.* at *20-21.

[66] *See id.* at *21-22 (citing People v. Weaver, 12 N.Y.3d 433, 441-45 (2009); United States v. Jones, 132 S. Ct. 945, 949 (2012)).

defendant's tweets under seal.[67]

[18] The line-drawing concerns that Twitter expressed 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*, a case in which the court held that "[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."[68]

[19] Some courts have concluded that individuals have "a reasonable expectation of privacy to [their] private Facebook information and messages."[69] Those courts, while recognizing the importance of properly understanding how Facebook works, distinguished between "private messaging" and posts to a user's Facebook wall.[70] Using privacy setting distinctions to determine social media users' constitutional rights may result in arbitrary line drawing that might evaporate as social media

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

[68] United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012).

[69] *See, e.g.*, R.S. v. Minnewaska Area Sch. Dist. No. 2149, Civ. No. 12-588 (MJD/LIB), 2012 WL 3870868, 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 v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (holding that "webmail and private messaging [are] . . . inherently private").

[70] *Minnewaska Area Sch. Dist. No. 2149*, 2012 WL 3870868, at *11; *Crispin*, 717 F. Supp. 2d at 991.

evolves. Indeed, with Facebook's customizable and post-specific privacy settings, a person who shares a message by posting it on another user's wall can actually make it as private as information shared via a Facebook message.[71]

[20] In addition, it remains uncertain whether, given the sheer breadth of information available in any particular social media account, one can successfully challenge search warrants for entire social media accounts for lacking sufficient limits or boundaries that would enable the government-authorized reviewing agent to ascertain which information the agent is authorized to review.[72] 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 through today's society may influence the privacy protections afforded to social media evidence in the future.[73]

VII. DEFENDING A CRIMINAL CASE WITH SOCIAL MEDIA EVIDENCE

[21] Defendants face more significant obstacles than the government when seeking exculpatory evidence from social media companies.[74] First,

[71] *See Timeline Privacy*, FACEBOOK, http://www.facebook.com/help/393920637330807/#!/help/393920637330807/ (last visited Jan. 20, 2013).

[72] *See In re* Applications for Search Warrants for Info. Assoc. with Target Email Address, No. 2:12-mj-08119-JPO, 2012 WL 4383917, at *5 (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).

[73] *See* United States v. Warshak, 631 F.3d 266, 284-85 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

[74] *See* Daniel K. Gelb, *Defending a Criminal Case from the Ground to the Cloud*, 27 CRIM. JUST. 28, 29 (2012).

defendants and their counsel do not share the government's freedom to sleuth for publicly available social media evidence, although counsel should have free access to anything his or her client produced or can access.[75] 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.[76]

[22] Second, defendants face additional hurdles when seeking to issue a third party subpoena.[77] Defendants may seek to subpoena social media companies for user information regarding the victim, the complaining witness, or another witness.[78] In those instances, in federal criminal proceedings, defendants must pursue such non-party discovery pursuant to

[75] *See* Zach Winnick, *Social Media an Ethical Minefield for Attorneys*, LAW360 (Apr. 13, 2012, 9:55 PM), http://www.law360.com/articles/329795/social-media-an-ethical-minefield-for-attorneys (noting 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).

[76] *See, e.g.*, PHILA. BAR ASS'N PROF'L GUIDANCE COMM., Op. 2009-02, at 1-3 (2009), *available at* 2009 WL 934623 (concluding that a social media friend request to a witness in the litigation by a third party for the purpose of gathering social media evidence is "deceptive" and in violation of ethical rules); N.Y. STATE BAR ASS'N, COMM. ON PROF'L ETHICS, Op. 843, at 2 (2010), *available at* 2010 WL 3961381 (noting that accessing publicly available social media evidence is permissible but 'friending" another party to do so is not); SAN DIEGO CNTY. BAR LEGAL ETHICS COMM., Op. 2011-02 (2011), *available at* http://www.sdcba.org/index.cfm?pg=LEC2011-2 (stating that ethics rules bar attorneys from making ex parte friend request of a represented party or 'deceptive' friend requests of unrepresented witnesses).

[77] In criminal litigation, the majority of evidence, electronic or otherwise, is collected by the government prior to trial, and Federal Rule of Criminal Procedure 16 does not require the government to produce such evidence unless it is being used in the government's case-in-chief. *See Warshak*, 631 F.3d at 327 (citing FED. R. CRIM. P. 16).

[78] *See* FED. R. CRIM. P. 17(c)(1).

Federal Rule of Criminal Procedure 17 and seek a court order allowing such a subpoena.[79] 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 or a government order.[80] In one high profile example of a defendant clearing such hurdles, 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 in addition to Mr. Martin's girlfriend's Twitter account.[81] Notwithstanding the order, Facebook and Twitter may challenge the subpoenas as Twitter so did in *People v. Harris*.

[23] Despite these challenges, criminal defendants may attempt to use novel methods of obtaining exculpatory social media evidence. For example, under *Brady v. Maryland* or *Giglio v. United States,* one may obtain a law enforcement officer's social media account records.[82] Moreover, courts may order jurors, witnesses, or third parties to produce or manipulate their social media information in unique and unprecedented

[79] *See* FED. R. CRIM. P. 17(a), (c)(3).

[80] *See* 18 U.S.C. § 2703(a), (c) (2006).

[81] Erin Fuchs, *A Jury Will Likely Scrutinize Trayvon Martin's Deleted Facebook and Twitter Accounts*, BUSINESS INSIDER (Oct.19, 2012, 2:56 PM), http://www.businessinsider.com/zimmerman-can-subpoena-social-media-2012-10.

[82] *See* Brady v. Maryland, 373 U.S. 83, 87 (1963) (holding that "the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material"); Giglio v. United States, 405 U.S. 150, 153-54 (1972) ("When the 'reliability of a given witness may well be determinative of guilt or innocence,' nondisclosure of evidence affecting credibility falls within this general rule [under *Brady*]." (citation omitted)) .

ways. For example, courts have: (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;[83] (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;[84] (3) recommended that an individual "friend" the judge on Facebook in order to facilitate an *in camera* review of Facebook photos and comments;[85] and (4) ordered parties to exchange social media account user names and passwords.[86] Such novel avenues of access to social media evidence may be considered when 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.

VIII. ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

[24] 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 creates hurdles to admissibility not faced with other

[83] Juror No. One v. Cal., No. CIV. 2:11397 WBS JFM, 2011 WL 567356, at *1 (E.D. Cal. Feb. 14, 2011).

[84] Katiroll Co. v. Kati Roll & Platters, Inc., Civil Action No. 10 3620 (GEB), 2011 WL 3583408, at *4 (D.N.J. Aug. 3, 2011).

[85] Barnes v. CUS Nashville, LLC, No. 3:09cv00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).

[86] *See, e.g.*, Gallion v. Gallion, No. FA114116955S, 2011 WL 4953451, 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 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010) (ordering plaintiff to produce Facebook and MySpace login credentials to opposing counsel for "read-only access").

evidence.[87] 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 in addition to considering how counsel will authenticate a tweet, Facebook posting, or photograph. Methods of authentication include presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it), searching the computer itself to see if it was used to post or create the information, or attempting to obtain the information in question from the actual social media company that maintained the information the ordinary course of their business.

[25] Notably, these same challenges face the government who must also consider the 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.[88] The government also performed a forensic examination of the hard drive and extracted 214 pages of Skype chats downloaded from the defendant's computer, which 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.[89] The logs "had a

[87] *See, e.g.*, Griffin v. State, 19 A.3d 415, 424 (Md. 2011) (recognizing "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator").

[88] United States v. Stirling, No. 1:11-cr-20792-CMA, at 2 (S.D. Fla. June 5, 2012), *available at* http://www.fuerstlaw.com/wp/wp-content/uploads/2012/06/altonaga-order-granting-new-trial1.pdf; *see U.S. District Court in Miami Orders New Trial Based on Discovery Violation for Electronically Stored Information*, FUERST ITTLEMAN DAVID & JOSEPH PL (June 25, 2012, 12:24 PM), http://www.fuerstlaw.com/wp/index.php/25/u-s-district-court-in-miami-orders-new-trial-based-on-discovery-violation-for-electronically-stored-information/.

[89] *Id.* at 2.

devastating impact" on the defendant because they contradicted many of his statements made during his testimony and he was convicted.[90] 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.[91]

[26] While both government and defense attorneys continue to 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 to give that evidence. For example, courts have ruled social media evidence as admissible where the content of the evidence contains sufficient indicia that it is the authentic creation of the purported user.[92] In *Tienda v. State*,

[90] *Id.*

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

[92] *See, e.g.*, People v. Lesser, No. H034189, 2011 WL 193460, at *4, *6 (Cal. Ct. App. Jan. 21, 2011) (finding officer's testimony that he cut and pasted portions of Internet chat transcript was sufficient for admissibility); People v. Valdez, 135 Cal. Rptr. 3d 628, 632-33, 635 (Cal. Ct. App. 2011) (upholding conviction where the court correctly admitted a trial exhibit consisting of printouts of defendant's MySpace page, which the prosecution's

the appellant was convicted of murder based in part on evidence that the prosecutors obtained after subpoenaing MySpace.[93] 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."[94] The Court of Criminal Appeals affirmed the trial judge's decision and concluded that the MySpace profile exhibits used at trial were admissible because they were a sufficient "indicia of authenticity" that "the exhibits were what they purported to be—MySpace pages for which the appellant was responsible for" the content.[95]

[27] In another recent case, a defendant was convicted of aggravated assault following a domestic dispute with his girlfriend.[96] At trial, the prosecution introduced Facebook messages sent from the defendant's account in which he indicated that he regretted striking his girlfriend and asked for her forgiveness.[97] The defendant denied sending the Facebook messages and argued that both he and his girlfriend had access to each

gang expert relied on in forming his opinion that defendant was an active gang member); People v. Fielding, No. C06022, 2010 WL 2473344, at *4-5 (Cal. Ct. App. June 18, 2010) (finding 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).

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

[94] *Id.* at 635.

[95] *Id.* at 647.

[96] Campbell v. Texas, 382 S.W.3d 545, 546 (Tex. App. 2012).

[97] *Id*. at 551.

other's Facebook accounts.[98] On appeal, the court, acknowledging that "electronic communications are susceptible to fabrication and manipulation," affirmed the trial court's ruling that allowed the state to authenticate the messages 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.[99] In another instance, a federal court found 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 it withheld ruling on the admissibility of the photos and whether they presented a risk of unfair prejudice.[100]

[28] 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 continue to be the subject of vigorous disputes between parties that may mean the difference between ultimate guilt and innocence.

IX. JURIES AND SOCIAL MEDIA

[29] Admissibility is just one challenge that the Internet and social media pose at trial. Another difficult issue relates to what information may be gathered about prospective jurors. At least one bar association has determined that attorneys may use social media websites to conduct juror

[98] *Id.*

[99] *Id.* at 549-50, 552.

[100] United States v. Drummond, No. 1:09-cr-00159, 2010 WL 1329059, at *2-3 (M.D. Pa. Mar. 29, 2010). The defendant ultimately entered a guilty plea, and the court did not make a final ruling on the admissibility of the photographs. Plea Agreement, *Drummond*, No. 1:09-cr-00159, 2010 WL7367722 (M.D. Pa. Nov. 29, 2010).

research as long as no communication occurs between the lawyer and the juror as a result of the research.[101] However, attorneys may not research jurors if that research results in the juror receiving a communication.[102] Third parties working for the benefit of or on behalf of an attorney must comport with the same restrictions as that attorney and, similarly to other ethical restrictions on defense counsel's ability to use social media as an investigative tool discussed *supra*, an attorney cannot use deception to gain access to a juror's website or to obtain information.[103]

[30] One of the most recent and challenging social media trends relates to jurors using wireless communication devices to look up a defendant's criminal record, conduct their own investigation into a case, post their opinions about the case on social media websites, or attempt to "friend" parties, lawyers, witnesses, or judges. In some instances, this conduct has resulted in mistrials and overturned convictions.[104] In other instances,

[101] *See* N.Y. STATE BAR ASS'N COMM. ON PROF'L ETHICS, Formal Op. 2012-2, at 5 (2012) *available at* 2012 WL 2304271; *see also* N.Y. CNTY. LAWYERS' ASS'N COMM. ON PROF'L ETHICS, Formal Op. 743 (2011), *available at* http://www.nycla.org/siteFiles/Publications/Publications1450_0.pdf (advising that it is ethical for lawyers to vet potential jurors by monitoring social network activity provided there is no contact or communication with the prospective jurors, and the lawyer does not seek to friend jurors, subscribe to Twitter accounts, send jurors tweets, or act in any way that alerts the jurors to the monitoring); Sluss v. Commonwealth, 381 S.W.3d 215, 227-28 (Ky. 2012) (adopting the model established by the New York County Lawyers Association).

[102] N.Y. STATE BAR ASS'N COMM. ON PROF'L ETHICS, Formal Op. 2012-2, *supra* note 101, at 5 (noting that even if an attorney unknowingly or inadvertently causes a communication with a juror, such conduct may run afoul of the Rules of Professional Conduct).

[103] *Id.* at 6-7.

[104] *See* Dimas-Martinez v. State, 385 S.W.3d 238, 246, 247, 249 (Ark. 2011) (reversing appellant's murder conviction and calling for a new trial when a juror tweeted several times during court proceedings, writing in one tweet, "Choices to be made. Hearts to be

such conduct has caused courts to conduct lengthy hearings to determine the impact of the juror's actions. For example, in *Sluss v. Commonwealth*, a defendant appealed his murder, assault, and evidence tampering convictions on the grounds that two members of the jury, including one who served as the jury foreperson, failed to indicate during voir dire that they had each "friended" the victim's mother through Facebook.[105] The Supreme Court of Kentucky, noting that being a "friend" on Facebook was not enough by itself to prove bias for disqualification as those "friendships" may be superficial, reversed and remanded the case with instructions to hold a hearing on whether the jurors should have been struck from the jury panel on the basis of their alleged social networking activity.[106] Finally, the inappropriate use of social media has led to stiff penalties for both jurors and attorneys.[107]

---

broken. We each define the great line," and later tweeting "Its [sic] over" before the jury announced its verdict).

[105] *Sluss*, 381 S.W.3d at 220-22.

[106] *Id.* at 223, 228-29; s*ee also* U.S. v. Ganias, Crim No. 3:08CR224(EBB), 2011 WL 4738684, (D. Conn. Oct. 5, 2011). In *Ganias*, the defendant filed a motion for a new trial on the eve of sentencing based on alleged juror improprieties. *Id.* at *1. The juror posted a variety of comments on the Facebook page, ranging from "Jury duty 2morrow. I may get to hang someone ... can't wait ..." before the presentation of the evidence, to "Guinness for lunch break. Jury duty ok today" during the three-week trial. *Id.* at *2. On the day of the verdict he posted "Guilty :)," and he also added a fellow juror as one of his Facebook friends. *Id.* Taken together, the defendant argued that the comments showed his Sixth Amendment rights were offended due to a biased juror. *Id.* at *1. When questioned, the juror assured the judge that he was merely "joking," and that he "absolutely was an impartial and fair juror." U.S. v. Ganias, Crim No. 3:08-CR-00224-EBB, 2011 WL 4738684, *3 (D. Conn. Oct. 5, 2011). The court found those statements presumptively honest, and denied the defendant's motion. *See id.* at *4.

[107] *See* John Barry, *Hillsborough Judge Vows to Send Prospective Juror to Jail*, TAMPA BAY TIMES, Oct. 11, 2012, *available at* http://www.tampabay.com/news/courts/criminal/hillsborough-judge-vows-to-send-prospective-juror-to-jail/1255802 (noting that prospective juror faces jail time for

[31] Both legislatures and courts have attempted to respond to these trends. For example, California adopted a new statute clarifying that jurors may not use social media and the Internet, such as texting, Twitter, Facebook, and Internet searches, to research or disseminate information about cases, and they can be held in criminal or civil contempt for violating these restrictions.[108] On August 21, 2012, a Judicial Conference Committee announced that it had created an updated model set of jury instructions to help judges discourage jurors from conducting research or communicating about their cases through social media.[109] The model instructions state:

> I know that many of you use cell phones, Blackberries, the Internet and other tools of technology. . . . You may not communicate with anyone about the case on your cell phone, through e-mail, Blackberry, iPhone, text messaging,

researching case and discussing it with the other jurors even after Tampa Bay court provided each member of the jury pool with a written order not to research or discuss the case and admonished and warned the jurors about the order at each break); Robert Eckhart, *Juror Jailed Over Facebook Friend Request*, HERALD-TRIBUNE, Feb. 16, 2012, *available at* http://www.heraldtribune.com/article/20120216/ARTICLE/120219626 (reporting that a court sentenced a juror to three days in jail for sending a Facebook message to the defendant and then posting "Score…I got dismissed!! apparently they frown upon sending a friend request to the defendant…haha," on Facebook after his dismissal from the jury); David Ovalle, *Lawyer's Facebook Photo Causes Mistrial in Miami-Dade Murder Case*, MIAMI HERALD, Sept. 13, 2012, *available at* http://www.miamiherald.com/2012/09/12/2999630/lawyers-facebook-photo-causes.html (reporting that a Miami judge declared a mistrial in a murder case after the public defender posted a photo of her client's leopard-print underwear on Facebook, which also led to the attorney's firing).

[108] *See* 2011 Cal. Stat. 181.

[109] *See Revised Jury Instructions Hope to Deter Juror Use of Social Media During Trial*, UNITED STATES COURTS (Aug. 21, 2012), http://news.uscourts.gov/revised-jury-instructions-hope-deter-juror-use-social-media-during-trial.

> or on Twitter, through any blog or website, including Facebook, Google+, My Space, LinkedIn, or YouTube. You may not use any similar technology of social media, even if I have not specifically mentioned it here.[110]

[32] The chair of the Conference Committee who provided the updated rules stressed that:

> The judges recommended that jurors frequently be reminded about the prohibition on social media before the trial, at the close of a case, at the end of each day before jurors return home, and other times, as appropriate. Jurors should be told why refraining from use of social media promotes a fair trial. Finally, jurors should know the consequences of violations during trial, such as mistrial and wasted time. Those recommendations are now part of the guidelines.[111]

X. CONCLUSION

[33] 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 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,

[110] JUDICIAL CONF. COMM. ON COURT ADMIN. & CASE MGMT., PROPOSED MODEL JURY INSTRUCTIONS: THE USE OF ELECTRONIC TECHNOLOGY TO CONDUCT RESEARCH ON OR COMMUNICATE ABOUT A CASE 1 (2012), *available at* http://www.uscourts.gov/uscourts/News/2012/jury-instructions.pdf.

[111] UNITED STATES COURTS, *supra* note 109.

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.