ETHICAL, EVIDENTIARY, AND CONSTITUTIONAL CONCERNS OF UTILIZING SOCIAL NETWORKING WEB SITES IN CIVIL AND CRIMINAL CASES: THE GOOD, THE BAD, AND THE UGLY

MARKA B. FLEMING *
JEAN T. WELLS **

I. INTRODUCTION

Social media, such as Facebook, Twitter and MySpace, are flowing into courtrooms across the country.[1] Indeed, during some trials, judges have allowed reporters to inform their audience about the status of a case through "tweets" or by posting live Twitter updates, straight from the trial. In a federal racketeering trial in March 2009, U. S. District Court Judge J. Thomas Marten allowed Ron Sylvester, a Wichita Eagle reporter in Kansas, to "tweet."[2] Similarly, in January 2009, Iowa federal Judge Mark Bennett permitted a Cedar Rapids Gazette reporter "to blog from a tax fraud trial, provided that she sit toward the back of the courtroom" to trigger the smallest amount of distraction from her typing.[3]

In addition to flowing into courtrooms through news media, such as reporters, social networking has become an important part of the process of litigating both civil and criminal cases.[4] Many lawyers have recently begun to access social networking

---

* J.D., Assistant Professor of Business Law, North Carolina A & T State University.
** J.D., CPA, Assistant Professor of Accounting, Howard University.

[1] *See* Tim McGlone, *Tangled in Their Own Webs*, VA. PILOT, July 13, 2009, at A1; Kate Wiltrout, *Sailor's Wife, Two Men Indicted on Murder-for-Hire Charges*, PILOTONLINE.COM, Feb. 23, 2008, http://hamptonroads.com/node/455173; Henry K. Lee, *Murder Suspect Identified Through Gang's MySpace Page*, S.F. CHRON., October 25, 2007, at B3; Brian Bergstein, *Cops Try to Knock Down Walls Between Web and Offline,* ASSOCIATED PRESS STATE & LOCAL WIRE, November 4, 2007; Shannon Awsumnb, *Social Networking Sites: The Next E-Discovery Frontier*, BENCH & BAR OF MINNESOTA, Vol. 66, No. 10, November 2009, *available at* http://www.mnbar.org/benchandbar/2009/nov09/networking.html.

[2] Ahnalese Rushmann, *Courtroom Coverage in 140 Characters*, NEWS MEDIA & LAW, Vol. 33, No. 2, Spring 2009, available at http://www.rcfp.org/news/mag/33-2/courtroom_coverage_in__characters_28.html ("But Marten's blessing signaled a key inroad for technology-enabled transparency in the notoriously camera-shy federal courts. Indeed, that the judge had to issue a formal order is itself a sign of how staunchly resistant the federal judiciary has been to live digital or recorded coverage from courtrooms."); *see also* Douglas L. Keene & Rita R. Handrich, *Online and Wired for Justice: Why Jurors Turn to the Internet (the "Google Mistrial")*, THE JURY EXPERT, *available at* http://www.astcweb.org/public/publication/article.cfm/1/21/6/Why-Jurors-Turn-to-the-Internet (last visited on Jan. 31, 2010).

[3] Rushmann, *supra* note 2.

[4] See *supra* note 1.

web sites for the purpose of litigating their cases.[5] And, surprisingly, courts have increasingly endorsed the use of this type of information in both civil and criminal cases.[6] Consequently, various legal issues have been raised including whether the information contained on social networking sites can be properly authenticated and whether it constitutes inadmissible hearsay evidence.[7] Another legal issue that has arisen as a result of the trend of utilizing this information in the litigation process involves whether obtaining this information from an individual's personal social network page violates the individual's Fourth Amendment right to be protected against unreasonable searches and seizures.[8] Furthermore, ethical questions have been raised regarding the manner in which this information can be acquired.[9]

In an effort to analyze this latest trend, the article will discuss social networking web sites and contemporary legal applications where these sites have been used in civil and criminal cases. It will also focus on some of the benefits of utilizing the information contained on these sites throughout the litigation process, along with the detrimental effects of popularizing the use of this information during litigation. Finally, the article will discuss potential legal objections that have arisen as a result of the use of this information--including ethical, evidentiary, and constitutional concerns.

II. SOCIAL NETWORKING WEB SITES

In general, humans have always craved social interaction, which was mainly limited to in person or over the telephone contact, until the 1990s when social networking sites provided people with another opportunity to interact socially.[10] As a matter of fact, the "advance in technology and the coming of age of electronic media" have led to the development of additional forms of communication including emails, texts and social networking sites."[11] Social networking sites have been

---

[5] *See* Justin Rebello, *Using Social Networks to Investigate Your Case*, LAWYERS USA, Aug. 11, 2008; Julie Kay, *Vetting Jurors Via MySpace*, Nat'l L. J., Aug. 11, 2008, *available at* http://nycrimbar.org/Members/Newsletter/2008-2009/VettingJurors-MySpace.pdf.

[6] *See* Thomas J. Prohaska, *Drunk Driver Gets into More Trouble after Posting Facebook Photo*, BUFFALO NEWS, Jan. 28, 2010, available at http://www.buffalonews.com/home/story/937238.html; Rebello, *supra* note 5.

[7] *See generally* Lorraine v. Markel Am. Ins. Co., No. PWG-06-1893 2007 U.S. Dist. LEXIS 33020 (D. Md. 2007); J. Shane Givens, Comment: *The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards*, 34 CUMB. L. REV. 95 (2003).

[8] *See generally* Ian Brynside, Note: *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applications*, 10 VAND. J. ENT. & TECH. L. 445 (2008); Givens, *supra* note 7, at 95.

[9] *See* Ken Strutin, *Pretexting, Legal Ethics and Social Networking Sites*, Oct. 5, 2009, *available at* http://www.llrx.com/features/pretexting.htm ("Yet, investigations that lead legal professionals into [social networking sites] raise questions about the ethical implications of surreptitious research.").

[10] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM., 13(1), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (last visited Feb. 27, 2010).

[11] *See* Laura McJimsey Randall, Comment: *The Guarantees of a Fair and Impartial Trial in the Midst of a Surge of Technological Advances: Should E-mails and Text Messages Be*

defined "as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[12] Further, they are considered to be "virtual communities on the Internet where people may go to find and 'connect with others who have similar interests.'"[13]

The first official social networking site was introduced in 1995 and it was called Classmates.com, which was designed to reconnect former school classmates.[14] During its infancy, however, Classmates.com did not offer its members the ability to create profiles, add individuals as friends, or view other members' profiles − important features which SixDegrees.com, another social networking site, included when it was launched in 1997.[15] Despite offering these features, SixDegrees.com lasted only three years and terminated its service in 2000.[16] During its operation, SixDegrees.com "promoted itself as a tool to help people connect with and send messages to others."[17] At that time, most individuals "did not have extended networks of friends who were online . . . and [e]arly adopters [of SixDegrees.com] complained that there was little to do after accepting Friend requests, and most users were not interested in meeting strangers."[18]

Between 1997 and 2004, several social networking sites were launched to satisfy a variety of niches including: LiveJournal ("a blogging platform and online community built around personal journals");[19]AsianAvenue, now called AsianAve.com ("[a] place to meet and connect with Asians around the country");[20] BlackPlanet.com ("the largest Black community online");[21] Friendster ("focused on helping people stay in touch with friends and discover new people and things that are important to them");[22] LinkedIn ("connect[s] the world's professionals to make them more productive and successful");[23] MySpace ("connecting people through personal

---

Admissible as Evidence Against a Defendant in a Criminal Trial?, 36 S.U. L. REV. 151, 152 (2008).

[12] Boyd & Ellison, *supra* note 10.

[13] Brynside, *supra* note 8, at 454 (quoting CYBER SAFETY GLOSSARY, *Definition of Social Networking Sites*, http://www.bsacybersafety.com/threat/social_networking.cfm).

[14] Boyd & Ellison, *supra* note 10; *see also* CLASSMATES.COM, http://www.classmates.com/ (last visited Feb. 27, 2010).

[15] Boyd, & Ellison *supra* note 10.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Our Company*, LIVEJOURNAL, http://www.livejournalinc.com/aboutus.php#ourcompany (last visited on Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

[20] ASIANAVENUE.COM, http://www.asianave.com/ (last visited Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

[21] BLACKPLANET.COM, http://www.blackplanet.com/ (last visited Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

[22] FRIENDSTER, http://www.friendster.com/info/index.php (last visited Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

[23] *About Us*, LINKEDIN, http://press.linkedin.com/about (last visited Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

expression, content, and culture");[24] and Facebook ("helps people communicate more efficiently with their friends, family and coworkers").[25] In particular, Friendster was launched in 2002 and because of its broad appeal – not to small niches – it dominated the scene until January 2004 when MySpace was launched.[26] By November 2004 − just ten months after its launch, MySpace had amassed five million members.[27] Nearly three years later, in March 2007, MySpace had "100 million monthly unique users worldwide."[28] One month after MySpace's launch, in February 2004, several Harvard University students launched Facebook, a social networking site that was initially limited to only Harvard University students. However, within a month of its launch, Facebook expanded "from Harvard to Stanford, Columbia and Yale."[29] Almost two years after its launch, Facebook had amassed "more than 5.5 million active users."[30] By October 2007, Facebook had 50 million users, nearly half that of MySpace at the time, making MySpace the dominant social networking site at the time.[31]

While the rivalry was continuing between MySpace and Facebook, Twitter was launched in March 2006 and has developed into a "real time short messaging service."[32] Postings, called "tweets" are limited to 140 characters − a limitation which "originated so tweets could be sent as mobile text messages."[33] This social networking site became more recognized in 2009 when a battle arose between CNN and Ashton Kutcher to determine which party could be the first to obtain one million followers on Twitter. [34] The rivalry garnered a significant amount of press and helped Twitter to become a more mainstream social networking site.[35]

---

[24] *MySpace Press Room*, MYSPACE, http://www.myspace.com/pressroom (last visited Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

[25] *Facebook Fact Sheet*, FACEBOOK, http://www.facebook.com/press/info.php?factsheet (last visited Feb. 27, 2010); *see also* Boyd & Ellison, *supra* note 10.

[26] *See* FRIENDSTER, *supra* note 22; *MySpace Press Room*, *supra* note 24; *see also* Boyd & Ellison, *supra* note 10.

[27] *Timeline*, MYSPACE, at http://www.myspace.com/pressroom?url=/timeline/ (last visited Feb. 27, 2010).

[28] *Id.*

[29] *See Facebook Fact Sheet*, *supra* note 25.

[30] *Id.*

[31] *Id.*; *see also Timeline*, *supra* note 27.

[32] *About*, TWITTER, http://twitter.com/about#about (last visited Feb. 27, 2010).

[33] *Id.*

[34] Interestingly, Kutcher eventually declared victory in April 2009. *See Kutcher's Twitter Flock first to Hit 1 Million*, ACCESS HOLLYWOOD, Apr. 17, 2009, http://www.msnbc.msn.com/id/30263363/; *see also* Jake Coyle, *Kutcher wins Twitter Battle with CNN*, ASSOCIATED PRESS ONLINE, Apr. 18, 2009, http://www.physorg.com/news159346471.html.

[35] Interestingly, Kutcher eventually declared victory in April, 2009. *See id; see also Audience Cheers as Oprah Writes First 'Tweet'*, ASSOCIATED PRESS, Apr. 17, 2009, *available at* http://www.msnbc.msn.com/id/30264819/ns/entertainment-celebrities/ (noting that the same week as the Twitter battle between CNN and Kutcher, Oprah jumped into the Twitter frenzy by sending her first tweet "ASHTON IS NEXT").

The number of people and the amount of time spent on social networking sites, like Twitter, Facebook and MySpace, are constantly increasing.[36] As of the Fall of 2009, those using social networking sites included the following groups of people: (1) 73 percent of "online American teens ages 12 to 17"; (2) 72 percent of online young adults ages 18-29; and (3) 40 percent of adults over 30.[37] Moreover, "visits to social networking Web sites increased 62 percent in September 2009 versus September 2008."[38] The extent and reach of social networking sites was evident in the 2008 presidential campaign and election when Senator Barack Obama became the first presidential candidate to utilize social networking sites to deliver his message and to organize political rallies.[39] As of February 2010, President Obama had 3.3 million followers on Twitter and 7.4 million Facebook fans.[40] Even the US Supreme Court has weighed in on the far reaching potential impact of social networking sites on politics in the case of *Citizens United v. Federal Election Commission*, where Justice Kennedy, writing for the majority, stated that soon "it may be that Internet sources, such as blogs and social networking Web sites, will provide citizens with significant information about political candidates and issues."[41]

III. LEGAL APPLICATIONS OF UTILIZING SOCIAL NETWORKING WEB SITES IN CIVIL AND CRIMINAL CASES

Lately, the information obtained from social networking web sites has been used for various purposes in litigating civil and criminal cases throughout the country.[42] One such use has been to assist parties during the investigatory phase of a case.[43] In fact, "[p]olice departments across the country are increasingly turning to social networking sites for clues to unsolved crimes", including crimes involving missing persons, robberies, sex crimes and even homicides.[44] For example, when detectives in Newport News, Virginia were investigating the April 2007 murder of Cory Voss, a Navy officer, their crime analyst expert on social networking

---

[36] *See* Amanda Lenhart, et al., *Social Media and Young Adults*, PEW INTERNET, Feb. 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.
[37] *Id.*
[38] *Facebook Visits Increased 194 Percent in Past Year*, EXPERIAN HITWISE, http://www.hitwise.com/index.php/us/press-center/press-releases/2009/social-networking-sept-09/ (last visited Feb. 27, 2010).
[39] On election day, Senator Obama had three million Facebook friends compared to Senator McCain's 600,000 friends. Matt Granfield, *How Social Media Won Obama the US Election*, MARKETING, Nov. 19, 2009, *available at* http://www.marketingmag.com.au/blogs/view/how-social-media-won-obama-the-us-election-865.
[40] Heather Hunt, *Wanted: A New First Tweeter for President Obama*, WASH. EXAMINER, Feb. 19, 2010, at 13, *available at* http://www.washingtonexaminer.com/economy/technology/84718647.html) (noting that the Democratic National Committee is seeking a "social networks manager" to manage Obama's three social networking sites of MySpace, Facebook and Twitter.).
[41] Citizens United v. Fed. Election Comm'n 175 L. Ed. 2d 753, 798 (Jan. 21, 2010).
[42] See *supra* note 1.
[43] *See* McGlone, *supra* note 1, at A1; Wiltrout, *supra* note 1.
[44] *See* McGlone, *supra* note 1, at A1.

discovered from MySpace that Voss' wife appeared to be having an affair with another man.[45] Based on the discovery of this information, Voss' wife, her boyfriend, and another MySpace friend were arrested for his murder.[46]

In a June 2007 case, the defendant, Matthew Cordova, was accused of robbing a University of Arizona student with a Tech 9 semi-automatic handgun.[47] After a police dispatcher found Cordova's MySpace account which had photos of Cordova holding what appeared to be a Tech 9, Cordova pled guilty to aggravated assault with a deadly weapon and was sentenced to five years in prison.[48] Similarly, information contained on a social networking site was utilized to identify a suspected gang member who was arrested in the slaying of a high school football player in Oakland, California. The defendant was identified through his picture on the gang's MySpace page.[49] Likewise, in 2007, a Newark, New Jersey detective tracked the alleged killers of three college students by searching MySpace pages maintained by the suspects and their friends.[50] Besides police officers, more and more attorneys are using social networking sites to uncover evidence about witnesses, victims and defendants and are utilizing this information to help them prepare their case such as serving as a tool to prepare for depositions.[51]

Information from social networking sites has also been utilized to investigate or vet potential jurors.[52] For instance, in *U.S. v. Hassoun*, the 2007 federal terrorism case of Jose Padilla and two other defendants, a juror was dismissed from the case after the defense attorneys' online search of jurors revealed that this juror had been dishonest on her jury questionnaire.[53]

Information obtained from social networking sites has also been used as admissible evidence against parties in civil and criminal proceedings to support case allegations. In practice, this evidence has helped parties defend criminal cases and

---

[45] *Id.*

[46] Notably, Voss' wife pled guilty to arranging the murder of her husband by hiring an assassin. *See id.*

[47] *See* Erica Perez, *Getting Booked by Facebook*, JSONLINE, http://www.jsonline.com/news/milwaukee/29260684.html (last visited on Feb. 8, 2010).

[48] *Id.*; *see also* Rebello, *supra* note 5. In September 2007, Laura Buys was driving drunk down on Highway 101 near Santa Barbara, California when she lost control of the vehicle and crashed killing her passenger. An office investigator for the Santa Barbara prosecutor did an Internet search on Buys and came across her MySpace page, which included a photo of Buys at a party during the sentencing phase of her trial sipping a class of wine and smiling. The page also included several entries about drinking and partying. The prosecutor submitted the MySpace page at the sentencing hearing and Buys was sentenced to two years in prison, which changed the tone or tenure of the case as it appeared during the criminal trial − before the MySpace page was submitted − where Buys appeared during this phase of trial to be deeply remorseful and as a result would not serve time.

[49] *See* Lee, *supra* note 1, at B3;Bergstein, *supra* note 1.

[50] Lee, *supra* note 1,at B3; *see also, Authorities Turn to Social Networking Sites to Make Cases*, ASSOCIATED PRESS STATE & LOCAL WIRE, September 16, 2007.

[51] *See Authorities Turn to Social Networking Sites to Make Cases*, THE ASSOCIATED PRESS STATE & LOCAL WIRE, September 16, 2007; *see also* Awsumnb, *supra* note 1.

[52] *See* Kay, *supra* note 5.

[53] *Id.*

pressure settlement and negate claims in civil cases.[54] An illustration of this is in the wrongful death action brought in 2005 by the family of a University of Texas student who died of alcohol poisoning during a fraternity initiation three years earlier.[55] During the case, the Texas court admitted as evidence pictures from the victim's Facebook page and a fifteen-second video of the fraternity members dragging the incapacitated victim upstairs to bed, where he eventually died.[56] Consequently, the Houston jury awarded $4.2 million to the victim's family.[57] Similarly, in July 2008, a Rhode Island court allowed as admissible evidence several pictures posted on a drunk-driving defendant's Facebook site showing him drinking at a Halloween party while wearing a prison garb labeled "Jail Bird."[58]

Admitting evidence from social networking sites has not been restricted to case allegations, but it has also been used to show that parties have failed to comply with court orders. [59] For example, a New York City criminal court ruled in 2008 that a MySpace "friend request" "constituted a violation of a no contact order of protection."[60]

---

[54] *See* John G. Browning, *What Lawyers Need to Know About Social Networking Sites*, DALLAS BAR ASSOC., Feb., 2009, available at https://www.dallasbar.org/members/headnotes_showarticle.asp?article_id=1530&issue_id=138 (Evidence from social networking sites has "help defend a murder case, pressure a settlement in a medical malpractice trial, negate a sexual harassment claim and even provide insight into prospective jurors.").

[55] Rebello, *supra* note 5.

[56] *Id.*

[57] *Id.*

[58] *Id.*; *see also* Browning, *supra* note 54 ("In Tucson, Arizona defense attorney Jesse Smith won an assault case after he impeached the state's star witness with video from the witness's own MySpace page, showing him beating up people and starting the brawl in which Mr. Smith's client had been implicated."); Molly McDonough, *Ind. High Court Allows MySpace Entry as Evidence in Murder Trial*, ABA J., October 16, 2009, *available at* http://www.abajournal.com/news/article/ind._high_court_allows_myspace_entry_as_evidence_in_murder_trial/ ("Saying that statements made on social networking sites are admissible as evidence of a defendant's character, the Indiana Supreme Court . . . upheld the conviction of a Northern Indiana man who beat his girlfriend's 2-year-old daughter to death in 2007.").

[59] *New York City Criminal Court Rules MySpace "Friend Request" Violates of Protection*, LAW. USA, March 10, 2008.

[60] "Members of MySpace receive and send messages known as 'friend request.' When a recipient gets a request, he or she has the option to approve or deny the request to maintain contact with that person online." In reaching its conclusion, the court said the following:

> The defendant should not be exculpated because she, instead of contacting her victim directly used the MySpace Mail Center Friend Request Manager. The defendant used MySpace as a conduit for communication prohibited by the temporary order of protection issued by the family court. The MySpace Friend Request falls within the court's mandate that, 'The defendant shall have NO CONTACT' with the former girlfriend.' While it is true that the person who received the request could simply deny the request to become 'friend' that request was still a contact and 'no contact' was allowed by the order of protection. It is no different than if the

Evidence obtained from social networking sites can also be helpful in the determination of the appropriate sentences imposed against a criminal defendant. A case in point was the evidence gathered from a Facebook page after Ashley Sullivan, a teenager, pled guilty to criminally negligent homicide and misdemeanor driving while intoxicated for killing her boyfriend who was a passenger in the car.[61] Weeks after Sullivan pled guilty to the charges; she visited Florida and posted a photo on her Facebook page entitled "Drunk in Florida."[62] At the subsequent sentencing in January 2010, the judge stated that he was troubled by Sullivan's conduct since the crash and "that's the reason for the [six month] jail sentence."[63] Similarly, a defendant, Jessica Binkerd, who had driven under the influence, resulting in a car crash that killed her passenger, was sentenced to five years and four months in prison after the prosecutor offered photos from Jessica's MySpace page following the accident showing her partying with friends and wearing an outfit with a liquor company's T-shirt and shot glasses.[64] It was reported that based on her MySpace page, the judge believed that Jessica had demonstrated no remorse for the accident.[65]

IV. POTENTIAL OBJECTIONS TO UTILIZING SOCIAL NETWORKING WEB SITES IN CIVIL AND CRIMINAL CASES

Although, as of late, courts have routinely admitted as evidence information contained on social networking sites, utilizing this type of information is not foolproof. Certainly, questions regarding the validity of its use exist and will likely become more common as this trend continues. In fact, potential objections to this information include the manner in which the information is obtained and the reliability of using of this information as evidence in court. Specifically, the legal objections involve ethical concerns, evidentiary concerns, and constitutional concerns. Each concern will be discussed independently.

> defendant arranged for any agent to make know to a claimant, 'Your former friend wants to communicate with you. Are you interested?'

Id.; *see also* Mann v. Department of Family and Protective Services, No. 01-08-01004-CV, 2009 Tex. App. LEXIS 7326 at *26 (affirming the trial court's decision to admit pictures from a mother's MySpace page to show that the mother--challenging the trial court's decree terminating her parental rights to her minor child and naming the Department of Family and Protective Services the child's sole managing conservator of the child--had drunk alcohol in violation of the court order that she refrain from criminal activity).

[61] *See* Prohaska, *supra* note 6.

[62] *Id.*

[63] *Id.*

[64] *See* Browning, *supra* note 54.

[65] *Id.*

A. *Ethical Objections to Obtaining Information from Social Networking Sites Through Trickery or Deceit*

Utilizing information from social networking sites in the litigation process can raise concerns about whether lawyers have engaged in ethical violations in obtaining this information.[66] On the whole, many of these sites provide their users with the ability to select privacy features, thereby enabling them to limit the access of the content of their social network page to select individuals. For instance, MySpace allows its users to "control what information is shared" and "who can view [the user's] profile";[67] Facebook users "have the ability to share and restrict information based on specific friends or friend lists";[68] and Twitter provides its users with the option of keeping their account public or "protecting the account to keep the updates private."[69]

1. Potential Ethical Violations of Obtaining Information through Trickery or Deceit

When a social network user chooses to exercise the available privacy features for his or her account, certain ethical issues can arise when an individual uses deception to obtain this information, such as becoming a "friend" in order to gain access to the social networking site. The precise issue of whether lawyers violate ethical rules of conduct by using trickery or deceit in order to obtain access to another individual's social networking site has not yet been addressed by the courts. Even so, the Philadelphia Bar Association Professional Guidance Committee (Committee) was asked this exact question by an inquiring attorney and the Committee provided its answer in a recent ethical opinion.[70]

The inquiring attorney deposed a witness, who was an 18 year old woman.[71] The witness was not a party to the litigation and she was not a represented party.[72] Nevertheless, this witness' testimony was adverse to the inquiring attorney's client.[73] During the course of the deposition, the witness revealed that she had both Facebook and MySpace accounts.[74] After discovering this information and upon the belief that the pages may contain relevant information concerning the witness' deposition

---

[66] *See* Strutin, *supra* note 9.
[67] *About Settings*, MYSPACE, http://www.myspace.com/Modules/ContentManagement/Pages/page.aspx?placement=privacy_settings (last visited Feb. 27, 2010).
[68] Facebook Fact Sheet, *supra* note 25.
[69] *Public vs. Private Accounts, Twitter*, http://help.twitter.com/entries/14016-public-vs-protected-accounts (last visited Feb. 27, 2010).
[70] Philadelphia Bar Association, Professional Guidance Committee, Opinion 2009-02, March 2009 at 1, available at http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*

testimony that could possibly be used to impeach the witness at trial, the inquiring attorney decided to visit Facebook and MySpace to access these accounts.[75] Upon viewing those accounts, the inquiring attorney discovered that the pages could only be obtained by the witnesses' permission.[76]

However, the inquiring attorney did not want to ask the witness for permission to provide him access to her social network accounts.[77] Instead, the inquiring attorney proposed as an alternative asking a third person − someone whose name the witness would not recognize − to go to the Facebook and MySpace web sites, contact the witness and seek to be her "friend" to obtain access to the information on the pages.[78] The third person in seeking to become the witness' friend would not disclose his or her affiliation or connection with the lawyer or the true purpose for which he or she was seeking access − "namely, to provide the information posted on the pages to a lawyer for possible use antagonistic to the witness."[79] The inquiring attorney asked the Committee whether the proposed course of action is permissible under the Rules of Professional Conduct and whether he could utilize the information obtained from the social network pages.[80]

In response to the inquiring attorney's question, the Committee indicated that the proposed action implicated several Pennsylvania Rules of Professional Conduct including Rule 8.4, governing *Misconduct*, which provides in pertinent part that "It is professional misconduct for a lawyer to: . . . (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation"[81] Specifically, the Committee explained that it believed that the proposed conduct "would violate Rule 8.4(c) because the planned communication by the third party to the witness is deceptive."[82] Moreover, the Committee indicated that the proposed action constituted a false statement of a material fact in violation of Pennsylvania Rule 4.1, governing *Truthfulness in Statements to Others*, stating in part that "[i]n the course of representing a client, a lawyer shall not knowingly . . . make a false statement of a material fact or law to a third person."[83] Thus, it was the opinion of the Committee, although only advisory, that the inquiring attorney should not obtain the information from the proposed manner.[84] The Committee did indicate that it thought that it was beyond its scope to decide whether this information could be used in litigation, but is a more appropriate question to be addressed as a matter of substantive and evidentiary issues by the court.[85] At the very least, this recent ethical opinion should remind lawyers to be cognizant of potential ethical violations that may exist in attempting to obtain access to such non-public material contained on social

---

[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.* at 2.
[81] *Id.* at 3.
[82] *Id.*
[83] *Id.* at 4.
[84] *Id.* at 6.
[85] *Id.*

networking sites through potentially deceptive means − like misrepresenting one's identity to become a "friend."[86]

Although the specific issue of whether it is unethical for lawyers to use trickery or deceit in order to obtain access to another individual's social networking sites has not been addressed by a court, promising guidance on this issue may be derived by analyzing the broader issue of whether it is ethically permissible for lawyers to use deceit in their investigations. In general, state bars − like Florida, Ohio and Vermont--frequently have rules of professional conduct prohibiting attorneys from engaging in professional conduct that constitutes fraud, deceit or misrepresentation.[87] Likewise, both the American Bar Association (ABA)'s Model Rules of Professional Conduct and its Model Code of Professional Responsibility prohibit an attorney from "engaging in conduct involving dishonesty, fraud, deceit or misrepresentation."[88] Nevertheless, a few jurisdictions have adopted exceptions for the use of deception in an investigation such as Florida, which allows an exception for government attorneys[89] and New York which permits an exception for prosecuting attorneys who supervise and advise undercover agents.[90]

A review of the relevant case law reveals that very few courts have actually addressed the specific issue of whether a lawyer's use of deceit in his or her investigation actually violates rules of professional conduct prohibiting an attorney from engaging in fraud, deceit or misrepresentation.[91] Even the American Bar Association has not yet addressed this particular issue. Yet, the Colorado Supreme Court did address this issue in the case of *People v. Pautler*, when a deputy district attorney intentionally posed as a public defender during telephone negotiations with a suspect who confessed to brutally killing three women and holding three others

---

[86] *See* Browning, *supra* note 54.

[87] *See, e.g.*, Fla. Bar Reg. R. 4-8.4 (In general, subsection (c) of Florida's Rule of Professional Conduct prohibits a lawyer from engaging in conduct involving dishonesty, fraud, deceit, or misrepresentation); Ohio Code Prof. Resp. DR 1-102(A)(4) (prohibiting conduct involving fraud, deceit, dishonesty, or misrepresentation); V.R.Pr.C. 8.4 (Subsection (c) of Vermont's Rule of Professional Conduct prohibits a member of the Bar from engaging in conduct involving dishonesty, fraud, deceit or misrepresentation. The rule was meant to reach only conduct that calls into question an attorney's fitness to practice law).

[88] MODEL RULES OF PROF'L CONDUCT 8.4(c); MODEL CODE OF PROF'L RESPONSIBILITY DR 1-102(A)(4).

[89] Florida's Rule of Professional Conduct provides that it shall be misconduct for attorneys to engage in "dishonesty, fraud, deceit, or misrepresentation" "except that it shall not be professional misconduct for a lawyer for a criminal law enforcement agency or regulatory agency to advise others about or to supervise another in an undercover investigation, unless prohibited by law or rule, and it shall not be professional misconduct for a lawyer employed in a capacity other than as a lawyer by a criminal law enforcement agency or regulatory agency to participate in an undercover investigation, unless prohibited by law or rule." Fla. Bar Reg. R. 4-8.4(c).

[90] *See* United States v. Parker, 165 F. Supp. 2d 431 (W.D. N.Y. 2001) ("Model Code of Prof'l Responsibility DR 1-102(A)(4) does not apply to prosecuting attorneys who provide supervision and advice to undercover investigations.")

[91] *See, e.g.,* People v. Pautler, 35 P.3d 571 (Colo. 2001); *see also* In re v. Gatti, 330 Ore. 517 (2000).

hostage and who had requested to speak with a public defender.[92] After reviewing the deputy district attorney's actions, the court concluded that the attorney violated Colorado Professional Rules of Conduct 8.4 (c) stating that an attorney's conduct "involving dishonesty, fraud, deceit or misrepresentation" constitutes professional misconduct.[93]

Similarly, in 2000, the Supreme Court of Oregon addressed a parallel issue in *In re v. Gatti*, by answering the question of whether there is an investigative exception which allows an attorney to use deceit in gathering information.[94] In this case, the lawyer's deception occurred when he telephoned two individuals and falsely represented himself as a medical professional. [95] Further, the lawyer failed to inform the individuals that he was actually a lawyer who was calling them for the purpose of gathering information.[96] The *Gatti* court held that the Oregon State Bar was not stopped from prosecuting the attorney and the court rejected the lawyer's contentions that the court should adopt an investigatory exception to Oregon's Profession Responsibility Disciplinary Rule (DR) 1-102 (A)(3) prohibiting conduct involving dishonesty, fraud, deceit or misrepresentation and DR 7-102 (A)(5) for knowingly making false statements of law or fact and Oregon Revised Statute § 9.527(4) for willful deceit or misconduct in the legal profession.[97]

In essence, the court found that the aforementioned disciplinary rules applied to all members of the Oregon State Bar without exception and therefore, the lawyer should be reprimanded for his actions during the telephone conversation with the two individuals.[98] However, in January 2002, the Oregon Supreme Court authorized an amendment to Oregon's DR 1-102, which states that "it shall not be professional misconduct for a lawyer to advise clients or others about or to supervise lawful covert activity in the investigation . . . provided the lawyer's conduct is otherwise in compliance with these disciplinary rules."[99]

2. The Admissibility of Information Obtained through Trickery or Deceit

An interrelated question to the issue of whether lawyers commit ethical violations by using trickery or deceit in their investigations is whether information obtained from such trickery or deceit is admissible in court. Here, there have been divergent decisions on this issue.[100] Some courts have admitted evidence obtained by a lawyer through trickery or deceit. In *United States v. Hammad*, the defendant, who was suspected of Medicaid fraud and arson, moved to suppress videotapes and

---

[92] Pautler, 35 P.3d at 577.
[93] *Id.* at 578.
[94] Gatti, 330 Ore. at 517.
[95] *Id.* at 521-22.
[96] *Id.*
[97] *Id.* at 532-33.
[98] *Id.* at 540.
[99] *See* OR. REV. STAT.DR. *§ 1-102(D) (2002*); *see also* Colleen E. McCullough, Student Commentary: *The Pursuit of a Prosecutorial Exception: In re Conduct of Gatti*, 27 J. LEGAL PROF. 217, 225 (2002).
[100] *See e.g.,* United States v. Hammad, 858 F.2d 834 (2nd Cir. 1998); Midwest Motor Sports v. Arctic Cat Sales, Inc., 347 F.3d 693 (8th Cir. 2002).

recordings obtained by an informant involved in a government investigation in violation of the ABA's Model Code of Professional Responsibility DR 7-104(A)(1), which "prohibits a lawyer from communicating with a 'party' he knows to be represented by counsel regarding the subject matter of that representation."[101] Despite the fact that the *Hammad* court refused to suppress the videotapes and recordings in violation of the professional rule of conduct, the court did note that it rejected "the government's effort to remove suppression from the arsenal of remedies available to district judges confronted with ethical violations."[102]

On the other hand, some courts refuse to admit evidence obtained from trickery or deceit.[103] In *Midwest Motor Sports v. Arctic Cat Sales, Inc.,* the court declined to admit evidence obtained by the defendant's investigator, at the direction of the defendant's attorneys, while the investigator was posing as a customer to solicit information from the plaintiff's employee without the knowledge of plaintiff's counsel.[104] As part of this investigation, the defendant's investigator recorded the conversations of the plaintiff's employee.[105] The court in *Midwest Motor Sport, Inc.* affirmed the district court's finding that the investigator's undercover ruse was used "to elicit damaging admissions" from plaintiff's employee "to secure an advantage at trial" and "[s]uch tactics fall squarely within ABA Model Rule 8.4(c)'s prohibition of 'conduct involving dishonesty, fraud, deceit or misrepresentation.'"[106] Also, the court in *Midwest Motor Sport, Inc.* determined that the district court did not abuse its discretion in imposing evidentiary sanctions against the defendant and its attorneys and the court held that the attorneys were ethically responsible for the investigator's conduct in communicating with the plaintiff's employee.[107]

B. *Evidentiary Objections to Using Information from Social Networking Sites in Court*

In addition to ethical concerns that may arise from using information contained on social networking sites in court proceedings, the admission of this type of evidence in these proceedings may also raise evidentiary concerns. The chief evidentiary concerns involve questions about the authenticity of this information and questions about whether the admission of this type of information will violate the evidentiary rules against hearsay. Notably, the framework that will be used in concentrating on the evidentiary concerns involved will be within the context of the Federal Rules of Evidence. Nevertheless, this framework should not limit the impact of the application of this information in state court proceedings since state courts have adopted evidence rules requiring the authentication of evidence and regulating

---

[101] Hammad, 858 F.2d at 836.
[102] *Id.* at 842.
[103] Midwest Motor Sports, 347 F.3d at 696.
[104] *Id.*
[105] *Id.* at 696.
[106] *Id*. at 700.
[107] *Id.* at 699.

hearsay evidence.[108] Moreover, given the limited number of cases focusing directly on evidentiary concerns involving information contained on social networking sites, in this section of the article, authenticity and hearsay concerns will encompass concerns regarding the more expansive category of evidence called "electronic evidence" − including emails, text messages, and information contained on web sites.[109]

---

[108] *See*, *e.g.*, ALA. R. EVID., 901 (2009) ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."); ALA. R. EVID., 801 (2009) ("Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."); KAN. STAT. ANN. § 60-464 (2008) ("Authentication of a writing is required before it may be received in evidence."); KAN. STAT. ANN. § 60-460 (2008) (Hearsay is defined as "[e]vidence of a statement which is made other than by a witness while testifying at the hearing, offered to prove the truth of the matter stated."); MONT. CODE ANNO., Ch. 10, Rule 901 (2009) ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."); MONT. CODE ANNO., Ch. 10, Rule 801 (2009) ("Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."); N.C. GEN. STAT. § 8C-1, Rule 901 (2009) ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."); N.C. GEN. STAT. § 8C-1, Rule 801 (2009)("Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."); *see also* Kendall Kelly Hayden, *The Proof is in the Posting, How Social Media is Changing the Law*, TX. BAR J., Vol. 73, No. 3, March 2010, at 189-90, *available at* http://www.texasbar.com/Template.cfm?Section=Texas_Bar_Journal1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=26428 ; People v. Clevenstine, 891 N.Y.S.2d 511, 514 (N.Y. App. Div., 2009) (holding authentication of information contained on the social networking site MySpace was established through the testimony from defendant's victims that "they had engaged in instant messaging about sexual activities with the defendant though the social networking site MySpace, an investigator from the computer crime unit of the [s]tate [p]olice related that he had retrieved such conversations from the hard drive of the computer used by the victims, a legal compliance officer of MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by the defendant and the victims, and the defendant's wife recalled the sexually explicit conversations she viewed in the defendant's MySpace account while on their computer."); In re J.W., No. 10-09-00127-CV, 2009 Tex. App. LEXIS 9830 at *8-9 (Tex. App. Dec. 30, 2009) (affirming the trial court's decision to allow into evidence about what a victim read on the defendant's MySpace page even though the victim admitted that she had no personal knowledge that the defendant had in fact typed this evidence on his MySpace page).

[109] *See* Givens, *supra* note 7, at 95 (quoting MANUAL FOR COMPLEX LITIGATION 21.446 (3d ed. 1995) ("'electronic evidence . . . may include information databases, operating systems, application programs 'computer-generated models, electronic and voice mail messages records, and other information or 'instructions residing in computer memory'"); *see*, *e.g.,* Clevenstine, 891 N.Y.S.2d at 514*;* In re J.W., No. 10-09-00127-CV, 2009 Tex. App. LEXIS 9830 at * 8-9; *see also* Hayden, *supra* note 108, at 189-90.

1. Authentication Objections

In attempting to admit electronic evidence, such as information obtained from social networking sites, a proponent must overcome objections made as to the authentication of this type of evidence. As Federal Rule 901(a), governing authentication, provides "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[110] The burden of proof for establishing authentication is not extremely high[111] and "[t]his burden is met when 'sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity.'"[112]

Generally, "evidence can be categorized into evidence that self-authenticates and evidence that requires authentication before it may be admitted."[113] Specifically, Federal Rule 902 lists those documents that are self-authenticating − meaning that they do not require extrinsic evidence of authenticity as a condition precedent to admissibility.[114] On occasion, electronic evidence has been determined to be self authenticating like the printouts of postings on the United States Census Bureau's website, which was ruled by the court in *Equal Employment Opportunity Commission v. E. I. DuPont De Nemours & Co*, to be self-authenticating under Federal Rule 902(5), which involves official publications, and "[b]ooks, pamphlets, or other publications purporting to be issued by public authority."[115]

However, since as a general rule, electronic evidence, such as information from social networking sites, will not be of the type that will be self authenticating, it will usually be necessary for the proponent attempting to offer this evidence to establish its authenticity from extrinsic evidence as directed by Federal Rule 901.[116] Federal Rule 901 sets forth an illustrative list of the means that can be used to authenticate evidence, but it is not an all inclusive list.[117] The first means under Federal Rule 901(b)(1) of authenticating evidence is through the testimony of a

---

[110] *See* FED. R. EVID. 901(a).

[111] *See*, *e.g.*, United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir. 1994) ("the burden of proof for authentication is slight"); United States v. Holmquist, 36 F.3d 154, 168 (1st Cir. 1994) ("the standard for authentication, and hence for admissibility, is one of reasonable likelihood"); United States v. Coohey, 11 F.3d 97, 99 (8th Cir. 1993) (noting that "the proponent need only demonstrate a rational basis for its claim that the evidence is what the proponent asserts it to be").

[112] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1154 (C.D. Cal. 2002) (quoting United States v. Tank, 200 F.3d 627, 629 (9th Cir. 2000)).

[113] John S. Wilson, Comment: *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1229 (2007).

[114] *See* FED. R. EVID. 902.

[115] Equal Emp. Opportunity Comm'n v. E. I. DuPont De Nemours & Co, No. 03-1605 SECTION: "R" (4), 2004 U.S. Dist. LEXIS 20753 (D. La. October 18, 2004); *see* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *65.

[116] *See*, *e.g.,* United States v. Safavian, 435 F. Supp. 2d 36, 39 (D.D.C. 2006) ("Because it is not appropriate for these e-mails to be admitted as self-authenticating under Rule 902 of the Federal Rules of Evidence, the Court turns to the authentication requirements set forth in Rule 901.").

[117] *See* FED. R. EVID. 901.

witness with knowledge that the matter is what it is claimed to be.[118] Courts considering the admissibility of electronic evidence frequently have acknowledged that it may be authenticated by a witness with personal knowledge set forth in Federal Rule 901.[119] For instance, in *St. Luke's Cataract's Laser Institute v. Sanderson*, the court stated that "[t]o authenticate printouts from a website, the party proffering the evidence must produce 'some statement or affidavit from someone with knowledge [of the website] . . . for example [a] web master or someone else with personal knowledge would be sufficient.'"[120]

Likewise, in *United States v. Safavian*, the court indicated that an email could be authenticated by a witness with knowledge that the email is what it is claimed to be.[121] Also, the *Safavian* court noted that electronic evidence can be authenticated under Federal Rule 901(b)(3), which involves the "[c]omparison by the trier of fact or by expert witnesses with specimens which have been authenticated." The court's endorsement of this means of authenticating emails was made evident when it said that email messages "that are not clearly identifiable on their own can be authenticated . . . by comparison by the trier of fact (the jury) with 'specimens which

---

[118] Other manners for authenticating evidence include the following: (2) Nonexpert opinion on handwriting. Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation; (3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated; (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances; (5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker; (6) Telephone conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone; (7) Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept; (8) Ancient: documents or data compilation. Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered; (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result; (10) Methods provided by statute or rule. Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority. FED R. EVID. 901 (b).

[119] *See, e.g.*, St. Luke's Cataract 's Laser Institute v. Sanderson, No. 8:06-cv-223-T-MSS, 2006 U.S. Dist. LEXIS (M.D. Fla. 2006).

[120] *Id.* at *5.

[121] United States v. Safavian, 435 F. Supp. 2d at 40 n.2 (D.D.C. 2006); *see also* Wady v. Provident Life & Accident Ins. Co. Am., 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining objection to affidavit of plaintiff's witness attempting to authenticate documents taken from the defendant's website because the affiant lacked personal knowledge of who maintained the website or authored the documents).

have been [otherwise] authenticated'--in this case, those emails that already have been independently authenticated under Federal Rule 901(b)(4)."[122]

Federal Rule 901(b)(4) has become one of the most common ways to authenticate emails and other electronic information such as text messages and contents on websites.[123] This section of Federal Rule 901 allows exhibits to be authenticated or identified by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[124] "'Use of this rule often is characterized as authentication solely by 'circumstantial evidence.'"[125] As to emails, they have regularly been authenticated through distinctive characteristics.[126] An illustration of this is the case of *United States v. Siddiqui*, where the court allowed the authentication of an email entirely by circumstantial evidence, including several factors the court considered to support the authenticity of the email such as the fact that the email bore the defendant's work email address; the contents of the email involved specific topics very familiar to the defendant; the email used the defendant's nickname; and there was witness testimony that the defendant spoke to these witnesses shortly after they received the email about the subjects contained in the email.[127]

Regarding information contained on Internet web sites, the courts' opinions as to the authenticity of this evidence has varied from complete opposition to allowing the admission of this evidence.[128] An example of a court's complete opposition to information contained on an Internet web site was the case of *St. Clair v. Johnny's Oyster & Shrimp, Inc*.[129] In this case--a case brought by a plaintiff for personal injuries while the plaintiff was employed as a seaman for the defendant-- the court, in deciding whether to grant the defendant's motion to dismiss, found the plaintiff's evidence obtained from the Internet to be totally insufficient to withstand the defendant's motion.[130] The court's reasoning was that any evidence obtained from the Internet was inadequate and in reaching this holding, the court stated the following:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that

---

[122] Safavian, 435 F. Supp. 2d at 40.
[123] *See* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *46.
[124] FED. R. EVID. 904(b)(4).
[125] Lorraine, 2007 U.S. Dist. LEXIS 33020 at *45 (quoting WEINSTEIN at §901.03[8])).
[126] *Id.*
[127] United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000); *see also*, Safavian, 435 F. Supp. 2d at 40; In Re F.P., a Minor, 878 A.2d 91, 94 (Pa. Super. Ct. 2005) (holding that the computerized instant messages were admissible and properly authenticated through the use of circumstantial evidence); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *45.
[128] *See*, *e.g.,* St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F.Supp.2d 773 (S.D.Tex. 2000); Perfect 10, Inc., 213 F.Supp.2d at 1146; U.S. v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000), *cert. denied*, 531 U.S. 973 (2000); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *77.
[129] St. Clair., 76 F. Supp. 2d at 775.
[130] *Id.*

> this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time.[131]

Also, in *United States v. Jackson*, the court refused to admit as authentic information obtained from an Internet website.[132] In particular, the *Jackson* court precluded the admission of certain web postings attributed to white supremacist groups because the court found the information to be "insufficiently authenticated."[133] Yet, the Jackson court did not imply--as the *St. Clair* court seemed to--that it viewed Internet evidence in general to lack authenticity. Instead, the court's holding was based on its determination that the criminal defendant had failed to show that the postings in which the groups appeared to claim responsibility for a series of racist mailings actually were posted by the groups as opposed to being posted by the defendant.[134]

Unlike the courts' findings in *St. Clair* and *Jackson,* the court in *United States v. Tank*, in focusing on the admissibility of electronic evidence, which encompassed chat room logs, held that the burden of proof required for authenticity was met where the producer of electronic evidence explained how he created these logs with his computer and stated that the printouts appeared to be accurate representations.[135] In effect, the government, the party offering the electronic evidence, was able to show the connection between the proffered evidence of the chat room logs and the party against whom the evidence was being offered, which was the defendant in this case.[136]

2. Hearsay Objections

Even if a proponent is able to meet the objection to authenticity of electronic information, such as information contained on social networking sites, the proponent may face another evidentiary hurdle in attempting to admit this evidence. This hurdle involves a showing that the electronic evidence does not constitute hearsay or is a hearsay exception. Under the Federal Rules of Evidence, hearsay "is an out-of-court statement offered in court to prove the truth of the matter asserted by the out-

---

[131] *Id.* at 774-75.
[132] Jackson, 208 F.3d at 637; *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *78.
[133] Jackson, 208 F.3d at 638.
[134] *Id.*
[135] Tank, 200 F.3d at 630; *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *82.
[136] Tank, 200 F.3d at 630-31.

of-court declarant."[137] However, under limited circumstances, courts will allow hearsay to be admitted into evidence as hearsay exceptions.[138] Interestingly, one of the chief purposes for the hearsay rule in criminal cases is to guarantee "the accused that all witnesses testifying against him will do so under oath and in person."[139] And, "another major justification for the inadmissibility of hearsay is that there is no opportunity to cross-examine the person making the out of court statement."[140]

Courts have on occasion held that electronic evidence is inadmissible hearsay evidence.[141] For example, in *Mary Kay v. Weber* − involving a trademark infringement suit brought by Mary Kay, a cosmetics manufacturer, against the defendants, an online cosmetics re-seller and its principals − the defendants objected to an exhibit containing numerous emails sent by customers complaining of used, damaged, or expired products.[142] After reviewing the emails, the court determined that the emails were "out-of-court statements offered for the truth of the matter asserted--the matter asserted being the matter complained of in the e-mail, i.e., that the products were old, damaged, or expired."[143] Contrary to the plaintiff's assertion, the court determined that the customer emails did not qualify under Rule 803(6) of the Federal Rules of Evidence governing business records because the complaints were not made by persons acting in the course of a regularly conducted business activity.[144] Therefore, since the court concluded that the customer emails were hearsay and were not covered by any exception, it held that these emails were inadmissible.[145]

But, the mere fact that the proponent is attempting to offer electronic evidence does not mean that this evidence will be found to be inadmissible hearsay. Generally, cases involving electronic information raise questions about whether the electronic information actually falls within the definition of hearsay.[146] In this regard, courts have held that electronic evidence is not considered to be "statements", in cases where the electronic evidence is "nonassertive or not made by a person."[147] Simply put, information generated by a machine does not constitute "statements" under the hearsay rule.[148] Instances of this type of electronic evidence

---

[137] FED. R. EVID. 801(a).
[138] *See* Randall, *supra* note 11, at 151.
[139] *Id.* at 153.
[140] *Id.*
[141] *See*, *e.g,* New York v. Microsoft, No. 98-1233 (CKK), 2002 U.S. Dist. LEXIS 7683 (D.D.C. Apr. 12, 2002) (holding that an email describing a telephone call did not qualify as a present sense impression because the email was not recorded while the event was being perceived or "immediately thereafter"); Mary Kay v. Weber, 601 F. Supp. 2d 839, 851 (N.D. Tex. 2009); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *133.
[142] Weber, 601 F. Supp. 2d at 851.
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *See* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *113 ("Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements" under Rule 801(a)").
[147] *See id.*
[148] *See id.*

have included: (1) the header or text of a fax;[149] (2) images and text posted on a web site;[150] and (3) computer generated records.[151]

Additionally, electronic evidence has been held to fall outside the definition of hearsay in those cases where the evidence is not being offered for the truth of the matter asserted, but is being offered for another purpose, like the case of *Perfect 10, Inc. v. Cybernet Ventures, Inc*., where the exhibits of defendant's website on a particular date did not constitute hearsay because they were offered to show trademark and copyright infringement not for the truth of the matter asserted.[152] *State v. Braidic* is another case in point where the electronic evidence being offered--the defendant's emails to the victim--was held to not constitute hearsay because the electronic evidence was not being offered to prove the truth of the statements, but instead was being offered to prove that the defendant asked the minor victim to state that she had lied about having sex with the defendant in order to get attention and the defendant had done nothing wrong.[153]

Courts have also determined that electronic information is excluded from the definition of hearsay under Federal Rule 801(d)(2) governing admissions against party opponents.[154] An example of a case where electronic evidence has been held to

---

[149] *See*, *e.g.*, United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) ("neither the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by 'a person,' so nothing 'said' by a machine . . . is hearsay.'"); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *113.

[150] *See*, *e.g.*, Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 U.S. Dist. LEXIS 20845 (N.D. Ill. Oct. 15, 2004) (ruling that images and text posted on website offered to show what the website looked like on a particular day were not statements and thus, was not governed by the hearsay rule); Perfect 10, 213 F. Supp. 2d at 1155 ("to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all--and thus fall outside the ambit of the hearsay rule."); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *114.

[151] *See*, *e.g.*, United States v. Rollins, No. ACM 34515, 2003 CCA LEXIS 303 at *24 (A.F. Ct.Crim.App. Dec. 24, 2003), *rev'd on other grounds* by No. 61 M.J. 338, 2005 CAAF LEXIS 906 (A.F. Ct.Crim.App. Feb. 8, 2005) ("The data at issue in this case were computer-generated, that is, created by the electrical and mechanical operation of the computer system. Thus, it was not an assertion of a person and was not hearsay."); People v. Holowko, 486 N.E.2d 877 (Ill. 1985) ("the printout of results of computerized telephone tracing equipment is not hearsay evidence of the type contemplated by section."); State v. Armstead, 432 So. 2d 837, 839-40 (La. 1983) ("the evidence in this case was generated solely by the electrical and mechanical operations of the computer and telephone equipment, and was not dependent upon the observations and reporting of a human declarant"); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *114.

[152] Perfect 10, 213 F. Supp. 2d at 1155.

[153] State v. Braidic, No. 28952-1-II, 2004 Wash. App. LEXIS 22 at *5 (Wash. App. Jan. 13, 2004) (The defendant was appealing his conviction of four counts of second-degree rape and one count of witness tampering.); *see also*, Lorraine, 2007 U.S. Dist. LEXIS 33020 at *119.

[154] FED. R. EVID. 801(d)(2); *see also* Siddiqui, 235 F.3d at 1323 (ruling that an email authored by defendant was not hearsay because it was an admission under Rule 801(d)(2)(A)); Safavian, 435 F. Supp. 2d at 43-44 (holding that an email sent by defendant himself was admissible as non-hearsay because it constituted an admission by the defendant under Rule 801(d)(2)(A) and as an "adoptive admission" under Rule 801(d)(2)(B)); Telewizja Polska USA, 2004 U.S. Dist. LEXIS 20845 at (holding that exhibits showing defendant's website as it

be an admission against a party opponent is the case of *MGM Studios, Inc. v. Grokster, Ltd*. brought on behalf of a group of record companies, movie studios and music publishers that filed a complaint against several defendants on the basis that the defendants' "file-sharing software contributed to massive infringement of copyrighted works owned by [p]laintiffs." [155] In particular, the electronic evidence objected to included emails authored by one of the defendants' corporate officers.[156]

Also, in *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, involving a contract dispute between a plaintiff and a defendant satellite television provider, both parties filed *motions in limine*.[157] Particularly, plaintiff's fifteenth *motion in limine* sought to preclude the defendant from introducing an exhibit to prove what the plaintiff's website looked like on various dates in 2001.[158] The plaintiff argued that the exhibit constituted double hearsay and as result, this information should not be admissible. The court in *Telewizja Polska USA* disagreed with the plaintiff's position because the court determined that "'[t]o the extent these images and text are being introduced to show the images and text found on these websites, they are not statements at all-and thus fall outside the ambit of the hearsay rule.'"[159] Moreover, the court held that the contents of the plaintiff's website were considered to be an admission of a party opponent and would not be barred by the hearsay rule.[160]

If electronic information is not determined to be excluded from the definition of hearsay, this evidence can only be admissible if it constitutes a hearsay exception under Federal Rule 803, which contains approximately twenty-three exceptions.[161]

---

appeared on a certain day were admissible as admissions against the defendant); Perfect 10, 213 F. Supp. 2d at 1155 (admitting an email sent by employees of the defendant against the defendant as admissions under 801(d)(2)(D)); State v. Franklin, 121 P.3d 447 (Kan. 2005) (holding that there was sufficient evidence to show that the sender of a text message was the defendant and as a result, the text message was admissible against the party opponent as a hearsay exception); Lorraine, 2007 U.S. Dist. LEXIS 33020 at *127.

[155] MGM Studios, Inc. v. Grokster, Ltd., 454 F.Supp. 966, 970 (C.D. Cal. 2006).

[156] Grokster, 454 F.Supp. at 973; *see also* Randall, *supra* note 11, at 160.

[157] Telewizja Polska USA , 2004 U.S. Dist. LEXIS at 20845.

[158] *Id.* at 16.

[159] *Id.* (quoting Perfect 10, 213 F.Supp.2d at 1155).

[160] *Id.* at 16-17.

[161] "[T]he twenty-three exceptions in Rule 803 may be grouped in three broad categories: Category 1 includes exceptions dealing with perceptions, observations, state of mind, intent and sensation (803(1) (present sense impressions); 803(2) (excited utterances); 803(3) (then existing state of mind, condition or sensation); 803(4) (statements in furtherance of medical diagnosis and treatment). Category 2 includes documents, records, and other writings (803(5) (past recollection recorded); 803(6) & (7) (business records); 803(8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12) (certificates of baptism, marriage and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) (ancient documents); 803(18) (learned treatises); 803(22) (judgments of conviction in a criminal case); and 803(23) (judgments in certain kinds of civil cases). Category 3 includes statements dealing with reputation (803(19) (reputation regarding personal or family history); 803(20) (reputation regarding custom, use and practice associated with land, and historically significant facts); and 803(21) (reputation regarding

Thus, even electronic evidence that constitutes hearsay may still be admissible as a hearsay exception. For instance, electronic information has been held to be admissible under Federal Rule 801(1) governing present sense impressions.[162] A case that demonstrates this point is the case of *United States v. Ferber*, where the court held that an email from an employee to his immediate supervisor regarding a phone conversation between the employee and the defendant was admissible and qualified as a present sense impression since the email was prepared shortly after the phone call occurred.[163] As well as constituting a present sense impression, electronic information has been held to be admissible under Federal Rule 801(b)(6) governing the business record exception to the hearsay rule like the case of *United States v. Fujii*, where the court held that computerized check-in and reservation records were admissible as business records since it was shown that these records were kept in the ordinary course of the business.[164] Besides, electronic information has on occasions been held to qualify under the public records exception to the hearsay rule such as in the case of *Lester v. Natsios*, where the court admitted the emails of the United States Agency for International Development, a public agency, and noted that "[r]ecords of public agencies such as those challenged by plaintiff are generally admissible."[165]

C. *Constitutional Objections to a Governmental Entity Gathering Information from Social Networking Sites*

As well as ethical and evidentiary concerns about using social networking sites in criminal and civil cases, a constitutional concern may arise as to whether the Fourth Amendment protection against unreasonable searches and seizures has been violated when a state actor,[166] like the police, gathers information from these sites.[167] Conceivably, this question would be raised if individuals owning social networking accounts are forced to surrender this information against their will or the information is obtained without the owner's permission. In order to show a violation of the

---

character within the community and among associates)." Lorraine, 2007 U.S. Dist. LEXIS 33020 at *128-129.

[162] *See*, *e.g.,* United States v. Ferber, 966 F. Supp. 90 (D. Mass. 1997); *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *133.

[163] Ferber, 966 F. Supp. at 98; *see also* Lorraine, 2007 U.S. Dist. LEXIS 33020 at *133.

[164] United States v. Fujii, 301 F.3d 535, 539 (7th Cir. 2002); *see also* Sea-Land Serv. v. Lozen, Int'l, LLC, 285 F.3d 808, 819-820 (9th Cir. 2002) (holding that a copy of an electronic bill of lading had been properly admitted as a business record since it was kept in the course of the plaintiff's regularly conducted business activity.); Lorraine, 2007 U.S. Dist. LEXIS 33020 at *148.

[165] Lester v. Natsios, 290 F. Supp. 2d 11, 30 (D.D.C. 2003); *see also,* E.I. DuPont De Nemours, 2004 U.S. Dist. LEXIS 20748 (holding that a table of information compiled by U.S. Census Bureau was admissible as a public record exception to the hearsay rule); Lorraine, 2007 U.S. Dist. LEXIS 33020 at *148.

[166] *See* Edwards-Flynn v. Yara, No. 08-0186 JB/ACT, 2009 U.S. Dist. LEXIS 49711 at *2 (D.N.M. March 31, 2009). ("Because the Court finds that the Defendants on this motion were not governmental entities or state actors, the Court will dismiss all claims against them for constitutional violations.").

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

Fourth Amendment, the party alleging the violation must show that there is a "reasonable expectation of privacy" meaning that the individual must show: (1) he or she "has . . . exhibited an actual (subjective) expectation of privacy and (2) there is an expectation of privacy that "society is prepared to recognize as reasonable."[168] However, as there are currently no cases addressing the constitutionality of obtaining information from social networking sites without the owner's permission, this could be described as "an emerging area of law."[169]

1. An Actual or Subjective Expectation of Privacy

Nevertheless, it can be presupposed that the court will first look at the question of whether the owner of the social networking account has exhibited an actual expectation or subjective expectation of privacy.[170] "A person may exhibit a subjective expectation of privacy by attempting to exclude the police or others from the area."[171] Therefore, when information contained on social networking sites is obtained without the social network account owner's permission, the question becomes whether the owner has taken precautions to exclude others from this area. For those social network sites that are not secured by some type of privacy protection, quite possibly this question could be answered in the negative and the court may be more prone to find that by failing to take any precautions to keep the information contained on the social network site private, the social network account owner has not exhibited any actual or subjective expectation of privacy.[172]

Even though the case did not involve a question regarding a reasonable expectation of privacy under the Fourth Amendment, a California appeals court in *Moreno v. Hanford Sentinel, Inc.,* held that by placing an article on her MySpace page, the author made her article available to anyone with Internet access.[173] And, in this case there was no indication that the author took any precautions to keep the information posted on her MySpace page private by using any privacy protections.[174]

---

[168] *See* Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J. concurring); *see also* Scott J. Smith, Note: *Thermal Surveillance and the Extraordinary Device Exception: Re-Defining The Scope of the Katz Analysis*, 30 Val. U.L. Rev. 1071, 1075 (1996) (The U. S. Supreme Court in *Katz v. United States* "established the principle that a 'search' occurs only when the government intrudes upon a person's 'reasonable expectation of privacy.'"); *see also* Florida v. Riley, 488 U.S. 445 (1989) (Applying the two-part test of whether an individual has established a subjective expectation of privacy and, if so, whether society would recognize this expectation as objectively reasonable.).

[169] *See generally* Brynside, *supra* note 8, at 458-59.

[170] *See* Katz, 389 U.S. at 360-61.

[171] *See* State v. Sletten, 664 N.W.2d 870, 876 (Minn. App. 2003), review denied 2003 Minn. LEXIS 622 (Minn. Sept. 24, 2003)("While a hotel guest may be protected under the Fourth Amendment, that right is not absolute; a hotel guest must first show a legitimate privacy interest."); *see also* U.S. v. Bolden, 545 F.3d 609, 620 (8th Cir. 2008) (affirming the district court's finding that the defendant exhibited no subjective expectation of privacy based on, among other factors, "failure to exclude others from entering the premises")."

[172] *See* Brynside, *supra* note 8, at 461

[173] Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr.3d 858 (Cal.App.5th 2009).

[174] *See id.*

The specific issue before the *Moreno* court was whether the author who posted the article on MySpace could state a cause of action for invasion of privacy or intentional infliction of emotional distress against the person who submitted that article for republication without the author's permission.[175] The court affirmed the trial court's ruling that the plaintiff-author failed to state a cause of action for invasion of privacy.[176] In reaching this holding, the court determined that the author's actions of posting the article on MySpace "opened the article to the public at large."[177] Accordingly, the court held that "no reasonable person would have an expectation of privacy" regarding the published article.[178]

2. A Reasonable Expectation of Privacy that Society is Prepared to Recognize as Reasonable

As to those social networking sites where the owners have placed some type of privacy protections, unlike that present in *Moreno*, courts may take the view that the individual has done enough to establish that there is a subjective expectation of privacy. Yet, a determination that the social network account owner has a subjective expectation of privacy does not end the inquiry under the Fourth Amendment. As a matter of fact, if the owner meets the first requirement, then the owner must also satisfy the more difficult showing of an expectation of privacy that "society is prepared to recognize as reasonable."[179] If social network account owners have failed to take precautions to exclude the information from others by using some type of privacy protections, a court would very likely conclude that there is no reasonable expectation of privacy.[180] In essence, the most viable cases on the issue of whether a social network account owner has an expectation of privacy for which "society is prepared to recognize as reasonable" may be those cases where the owner has taken precautions to exclude the information from others by using some type of privacy protections.[181]

But, the privacy protections may not be enough. A court could hold that social network account owners lose their reasonable expectation of privacy by placing information on the Internet, which may be viewed as being within the public domain.[182] In the case of *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, although the issue of whether the privacy settings are enough to protect a social network account owner under the Fourth Amendment was not addressed, the federal district court was asked to consider the question of whether a party to a lawsuit could discover private email messages on two social network accounts without a search

---

[175] *Id.* at 861.
[176] *Id.* at 864.
[177] *Id.* at 863.
[178] *Id.* at 862.
[179] *See* Katz, 389 U.S. at 360-61.
[180] *See* Wilson, *supra* note 113, at 1233-34.
[181] *See id.* at 862.
[182] *See* Brynside, *supra* note 8, at 461 (citing Michael Whiteman, *The Impact of the Internet and Other Electronic Sources on an Attorney's Duty of Competence under the Rules of Professional Conduct*, 11 ALB. L.J. SCI. & TECH. 89, 97 (2001)).

warrant or a letter of consent by the owner of the accounts.[183] The facts present in this case were that the defendants of a sexual harassment action moved to compel email communications on two MySpace accounts set up by the plaintiff.[184] In one of the MySpace accounts, the plaintiff allegedly identified herself as a 39 year old single female who did not want kids, while on the other MySpace account the plaintiff identified herself as a 39 year old married female with six children and indicated that she loved children.[185] The defendants wanted to offer evidence of the information contained on the MySpace accounts to show that the plaintiff was a willing participant who actively encouraged the sexual communications and conduct with her alleged harassers.[186] Moreover, the defendants contended that this evidence could contain statements made by the plaintiff and witnesses "about the subject matter of [the] case which could presumably constitute admissions by [p]laintiff or which could potentially be used to impeach the witnesses' testimony."[187]

The court in *Mackelprang* concluded that the defendants were entitled to receive the information in the email messages that related to the plaintiff's emotional distress claim, but held that the proper method for obtaining this information "is to serve upon [p]laintiff properly limited requests for production of relevant email communications" as opposed to the method used by the defendant of serving a subpoena on Myspace.com to produce all records for these two MySpace accounts set up by the plaintiff.[188] Furthermore, the court did note that although it was denying the defendants' motion to compel, the order did not prevent the defendants from "serving such discovery requests on [p]laintiff to produce her Myspace.com private messages that contain information regarding her sexual harassment allegations in this lawsuit or which discuss her alleged emotional distress and cause thereof."[189] In other words, the court did not hold that the information contained on the plaintiff's Myspace accounts were undiscoverable because the plaintiff had marked these accounts as private.[190]

Notwithstanding the foregoing analysis, there is no certainty as to how a court would actually decide the issue of whether a governmental entity violates a social network account owner's Fourth Amendment rights by obtaining information contained on the owner's social network site without his or her permission and any deduction is currently unverifiable. In fact, one author, Carly Brandenburg, stated in her Note titled *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare* that "[n]o clear answer can yet be gleaned from legal precedent as to whether the Facebook users and other social networkers have a reasonable expectation of privacy in their profiles and posted material."[191] Moreover,

---

[183] Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc., No: 2:06-cv-00788-JCM-GWF, 2007 U.S. Dist LEXIS 2379 at*5 (D. Nev. January 9, 2007).
[184] *Id.* at *4.
[185] *Id.* at *5-6.
[186] *Id.* at *20.
[187] *Id.*
[188] Id. at *5, *26.
[189] *Id.* at *26.
[190] *Id.*; *see also* Awsumnb, *supra* note 1.
[191] Carly Brandenburg , Note: *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare*, 60 FED. COMM. L.J. 597, 604 (2008).

Brandenburg acknowledged that there is no clear consensus among the courts on the question -- that parallels the situation where information is obtained without the permission of the social network account owner--of whether a person retains a reasonable expectation of privacy when "the information [the] person intended to keep private was intentionally shared with some but also fell in the hands of unintended recipients."[192] Nevertheless, while the issue as to whether there is a reasonable expectation of privacy has yet to be resolved, as the trend of utilizing information contained on social networking sites continues to become more popular, this issue will probably be addressed by courts throughout the country in the near future.

V. THE IMPACT OF UTILIZING SOCIAL NETWORKING WEB SITES IN CIVIL AND CRIMINAL CASES

In spite of the potential objections to utilizing social networking sites in the litigation process, it can be argued that the use of this information can be beneficial to this process. As previously discussed in Section III. of this article, social networking sites can be used for numerous purposes during the litigation process, including improving this process by assisting parties in locating witnesses and providing additional sources of potential evidence.[193] And, in many cases this tool is revealing vital evidence like the picture posted online by the killer of a seventeen year old Virginia college student connecting the killer to the victim,[194] or the declaration by a young man in an Indiana case on his MySpace page stating, "I just killed two cops."[195]

Further, information contained on social networking sites has provided evidence that has proven to be "beneficial to some victims, especially children."[196] In *Dexter v. Dexter*, the court of appeals upheld the trial court's decision to admit a mother's MySpace postings to consider the probable effect some of the mother's personal choices would have on her daughter, including admissions in blogs that she practiced sadomasochism, was bisexual, a pagan and used drugs.[197] Based on these

---

[192] *Id.* at 604.

[193] *See* Rebello, *supra* note 5 ("These sites can also be a huge boon for attorneys who are trying to locate a missing witness or, in the case of an estate planning case, a missing heir.").

[194] Brian Bergstein, Cops *Try to Knock Down Walls Between Web and Offline*, ASSOCIATED PRESS STAT & LOCAL WIRE, Nov. 4, 2007, available at http://abclocal.go.com/ktrk/story?section=news/technology&id=5735814.

[195] Notably, one of the two officers described in this MySpace site survived the shooting. *Cops Turn to Facebook, MySpace Profiles to Solve Crimes*, BREAKING NEWS, Nov. 04 2007, *available at* http://news.bn.gs/article.php?story=20071104122053837; *see also* Bergstein, *supra* note 1.

[196] Hayden, *supra* note 108, at 190.

[197] Dexter v. Dexter, No. 2006-P-0051, 2007 Ohio App. LEXIS 2388 at *13-21 (Ohio Ct. App. May 25, 2007); ; *see also* Hayden, *supra* note 108 at, 190.; Mann, No. 01-08-01004-CV, 2009 Tex. App. LEXIS 7326 at *26; In re K.E.L., No. 09-08-00014-CV, 2009 Tex. App. LEXIS 1382 at *12-14 (Tex. App. Feb. 26, 2009) (affirming the trial court's decision, in determining which parent should serve as the person with the right to designate the child's primary

admissions, the trial court determined that the daughter's best interests could be adversely affected by the mother's lifestyle and therefore, it granted the father custody of the child.[198]

Information contained on social networking sites can also improve the litigation process by helping prepare witnesses for depositions and trial testimony.[199] Indeed, it has been suggested that defense attorneys may do a disservice to their clients "by not at least checking with them to see if they maintain a Web page used for social networking, in addition to the standard methods of digging up dirt."[200] Arguably, as the number of people socially connecting continues to increase, the information posted on these social networking sites could very possibly become an essential weapon to the litigants in both civil and criminal cases.[201]

The counterargument to the contention that social networking sites improve the litigation process is the assertion that the popularization of the use of this information during the litigation process is harmful to this process. This argument may be viewed as compelling in those cases where social networking sites have been misused by the parties involved in the process, including judges, lawyers, witnesses, parties, and jurors.[202] In effect, misuse of social networking sites can have detrimental effects on the litigation process. For example, when judges misuse social networking sites, this can taint the entire litigation proceeding. An application of a judge's misuse of a social networking site is the 2009 case of a North Carolina judge involved in a custody and support case who was reprimanded and transferred to another jurisdiction for "friending" a lawyer who appeared before him through Facebook and "posting and reading messages about the litigation, and accessing the website" of the other lawyer who was not a Facebook friend of the judge.[203]

---

residence, to admit the contents of the father's MySpace page that contained sexually-oriented statements that he agreed he had made on the page).

[198] Dexter v. Dexter, No. 2006-P-0051, 2007 Ohio App. LEXIS 2388 at *13-21

[199] *See Authorities Turn to Social Networking Sites to Make Cases*, *supra* note 50.

[200] Rebello, *supra* note 5 (noting that "defense attorneys do their clients a disservice by not at least checking with them to see if they maintain a Web page used for social networking").

[201] *See* Alex Lundberg, *Social Web Sites Becoming New Tool for Lawyers Seeking Information*, MICH. LAW. WEEKLY, July 27, 2009, available at http://www.allbusiness.com/society-social/families-children-family-law-child/12600152-1.html ("The personal information people post on Web sites like MySpace, Facebook and Twitter is becoming a new weapon in the family lawyer's arsenal as more people make connections via social networking services." There have been custody cases "where a parent's claims of propriety and worthiness have been undermined by pictures of him or her drunk and partying - pictures that parent often posted online personally.").

[202] John Schwartz, A Legal Battle: Online Attitude vs. Rules of the Bar, N. Y. TIMES, Sept. 12, 2009, *available at* http://www.nytimes.com/2009/09/13/us/13lawyers.html?_r=4; *see also*, Keene & Handrich, *supra* note 2.

[203] *See* N. C. Judicial Standards Comm'n Inquiry No. 08-234 (2009), *available at* http://www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf ; *see also* Debra Cassens Weiss, *Judge Reprimanded for Friending Lawyers and Googling Litigant*, ABA J., June 1, 2009, *available at* http://www.abajournal.com/news/article/judge_reprimanded_for_friending_lawyer_and_googling_litigant/ ; *cf.,* Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches #ABAChicago*, ABA J., July 31, 2009, *available at*

Misuse of social networking sites by lawyers can have an equally damaging effect on the litigation process. Indeed, "[s]ocial networking presents many new ways for lawyers to [inadvertently] reveal client information . . . and [l]apses in confidentiality can occur on a firm's Web site and client intake forms, in emails and attachments, on lawyer blogs, bulletin boards, chat rooms, and listservs, and in many other communication forms."[204] Lawyers' misuse of social networking sites have also lead to disciplinary actions like the Florida attorney who was reprimanded and forced to pay sanctions in the amount of $1,200 for blogging about a judge whom the attorney called an "evil, unfair witch" or the Illinois assistant public defender who blogged about a "Judge Clueless" and "thinly veiled the identities of clients and confidential details of a case," resulting in her job loss after nineteen years with the state. [205]

Inappropriate use of social networking sites by parties, witnesses and jurors[206] can provide possible grounds for a mistrial or a new trial.[207] An example of jurors' misuse of social networking sites arose during the recent embezzlement trial of Sheila Dixon, the former mayor of Baltimore, Maryland, which was held in November 2009.[208] Although Dixon sought a mistrial after it was revealed that five jurors had communicated through Facebook during the three-week trial, no decision on her allegations of juror misconduct was ever reached since Dixon and the prosecutors were able to reach a plea agreement.[209]

Remarkably, the increase in the frequency of jurors misusing social network sites, like that present in Dixon's case, has resulted in courts updating their juror

---

http://www.abajournal.com/news/article/facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago/ (A judge visited a lawyer's social networking site after the lawyer requested a continuance due to a death of her father and saw pictures of the lawyer partying around the same week as the death.).

[204] Steven C. Bennett, *Ethics of Lawyer Social Networking*, 73 ALB. L. REV. 113, 118-19 (2009) (citing Cydney Tune & Marley Degner, *Blogging and Social Networking: Current Legal Issues, in Information Technology Law Institute 2009: Web 2.0 and the Future of Mobile Computing* 113, 130 (2009)).

[205] *See* Schwartz, *supra* note 202; *see also* Keene & Handrich, *supra* note 2.

[206] *See*, *e.g.,* Julie Bykowicz, *5 Dixon Jurors Recalled as Witnesses*, BALTIMORE SUN, Dec. 30, 2009, *available at* http://articles.baltimoresun.com/2009-12-30/news/bal-md.dixon30dec30_1_juror-misconduct-new-trial-arnold-m-weiner (After her trial for embezzlement on November 9, 2009 to December 1, 2009, Sheila Dixon, the then mayor of Baltimore was sought a mistrial after it was revealed that five jurors had "communicated through Facebook during the three-week trial."); David Kravets, *Jurors: Stop Twittering*, CNN TECH , available at http://www.cnn.com/2010/TECH/02/10/wired.jurors.twitter/index.html (last visited on Feb. 28, 2010) ("[T]here was a call, although unheeded, for a mistrial when a juror was discovered tweeting and publishing trial updates on Facebook in the prosecution of Vincent Fumo, a former Pennsylvania state senator.").

[207] *See*, *e.g.*, Del Quentin Wilber, *Social Networking Among Jurors is Trying Judges's Patience*, WASH. POST, Jan. 9, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/01/08/AR2010010803694.html.

[208] *Id.*

[209] *Id.*

instructions to reflect this "new digital age."[210] As a matter of fact, in February 2010, the Judicial Conference of the United States, the policy-making body of the federal courts, proposed "that judges clearly inform jurors they must not electronically discuss cases they are hearing" and released model instructions stating the following:

> You may not communicate with anyone about the case on your cellphone, through e-mail, Blackberry, iPhone, text messaging, or on Twitter, through any blog or website, through any internet chat room, or by way of any other social networking websites, including Facebook, MySpace, LinkedIn and YouTube.[211]

Considering both the arguments for and the arguments against utilizing social networking sites in civil and criminal cases, the proposed supposition is that this information should be used in the litigation process. The premise for this supposition is that social networking sites can serve as a valuable tool in the litigation process if this tool is used wisely. In essence, as long as the information contained on social networking sites is not misused, the impact of utilizing this information during the litigation process can be beneficial to all parties involved in this process.

VI. CONCLUSION

Recently, parties involved in the litigation process have begun using social networking web sites in both criminal and civil cases. As a result of this growing trend, several challenges have arisen regarding the validity of this information. These include ethical, evidentiary and constitutional challenges. The ethical challenges surround the manner in which this information is obtained, while evidentiary challenges involve whether this information can be authenticated and whether it constitutes inadmissible hearsay evidence. Finally, the constitutional challenge implicated when social networking sites are utilized is whether a governmental entity violates a social network account owner's Fourth Amendment rights by obtaining this information without the owner's permission.

Based on the existing case law, it can be inferred that under certain circumstances information contained on social networking sites can be authenticated

---

[210] *See* Eric P. Robinson, *Michigan High Court Sends Message to Tweeters*, CITIZENS MEDIA LAW PROJECT, Jul. 7, 2009, *available at* http://www.citmedialaw.org/blog/2009/michigan-high-court-sends-message-tweeters (noting that "the Michigan Supreme Court has adopted a new rule requiring judges to admonish jurors to not use electronic communication devices during trial, and not to use them during breaks to comment or conduct research on the case"); Robert K. Gordon, *Facebook, Twitter Causing Judges to Amend Jury Instructions*, BIRMINGHAM NEWS, Oct. 20, 2009, *available at* http://www.al.com/news/birminghamnews/index.ssf?/base/news/1256026558309710.xml&coll=2 ("After U.S. District Court Judge Scott Coogler seated jurors to hear the case of Birmingham Mayor Larry Langford, he gave them an extra instruction: no tweeting during the trial.").

[211] Kravets, *supra* note 206.

and will not be barred as inadmissible hearsay evidence. However, there are no clear answers on the ethical and constitutional challenges as this is an "emerging area of the law"[212] that is presently undetermined. Yet, it can be supposed that these issues will be resolved in the near future as the trend of using social networking sites in civil and criminal cases becomes more popular. While there are both recognizable benefits and detriments to using social networking sites in litigation, the question of whether the information contained on these sites should be used is a debatable issue, with little possibility of being resolved in the near future.

[212] *See generally* Brynside, *supra* note 8, at, 458-59.