

The Discoverability of Social Media

*Bonnie Roach**

ABSTRACT

Social media is now an integral part of our culture. Millions of people maintain contact with each other and share the day-to-day occurrences of their lives in both text and pictures. Along with the increase sharing of information, which many times is meant to be viewed only by friends and family, there is an increasing concern that the shared information may be viewed by others who are not normally permitted to see the poster's materials. Some invasions of privacy are for nefarious purposes, but some are done with the blessings of the court.

An example of this is when parties to a lawsuit are involved in the discovery phase of trial. Social Media Sites (SMS) such as Facebook, contain a possible plethora of evidence that is easily available within the site. However, as is the case for obtaining and admitting all evidence, the party requesting the SMS data must make a showing of its probative value, especially if that party is a public employee or the information itself is placed in the "private" areas of the SMS.. This paper investigates some of the emerging concerns regarding the discovery of social media, such as gaining access to SMS evidence, demonstrating probative value; authentication of SMS data in private versus more public areas of the SMS and some of the pitfalls attorneys may encounter in using SMS data such as spoliation.

INTRODUCTION

It would be an understatement to say that social media, such as Facebook, is one of the primary ways we all stay in touch with relatives, friends and sometimes, complete strangers. More and more individuals are using social media. Some estimate that 72% of all adults use social networking sites²²⁷ and that there are 1.23 billion users of Facebook.²²⁸ All of those users are using their social media accounts to send each other messages, post pictures, or share other postings on a wide variety of topics. Users of social media believe that their postings are protected from scrutiny from the outside world due to the various privacy settings that can be utilized by the user. Social media users are lulled into a false sense of security that the postings they create will only be viewed by those individuals who have permission to see these items by the individual.

The illusion of privacy is not the only misperception that SMS users may have. Users of SMS erroneously believe that only permitted individuals have the ability to view the contents of the users' SMS account. It is becoming more and more common for SMS material to be used in various types of legal actions, including employment law issues. Social media is proving to be a goldmine for attorneys seeking evidence on behalf of their clients and the news media is full of

* Ohio University

²²⁷ Amanda Lenhart et al., *Social Media & Mobile Internet Use Among Teens and Young Adults*, PEW INTERNET (Feb.3, 2010), [http://www.pewinternet.org/\[#x007E\]/media//Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplevels.pdf](http://www.pewinternet.org/[#x007E]/media//Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplevels.pdf).

²²⁸ Smith, Craig, *How Many People Use 415 of the Top Social Media, Apps and Tools*, Digital Marketing Ramblings: The Latest Marketing Strategies, Tips, Trends and Technology. (March, 2014). <http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/3/#.U0oTwsf1bzM>

stories where social media was used to resolve various legal issues. Even the recent case of racial discrimination that was filed against FoodNetwork star Paula Deen and her brother involved the discovery of electronic tweet data.²²⁹ Jackson had alleged that racial slurs were exchanged amongst the employees of the Lady and Sons, the restaurant owned and run by Deen. Attorneys for the defense were seeking the tweets of the plaintiff because they were considered important evidence in establishing whether racial discrimination had occurred. The judge rejected the motion saying that there was no relevance of the tweets to the case at hand and the request itself was overbroad.²³⁰

The Deen case illustrates the fact that SMS data that can be used as evidence, but secondly, SMS must be relevant to the case at hand. As more individuals use SMS, the more likely it is that evidence from these sites will become very helpful, especially in employment law litigation. Employers' use of social media and other electronic media is not uncommon. For many years now, employers have relied on SMS and electronic monitoring to detect productivity issues (uncovering prohibited activities such as web surfing and paying solitaire) to using electronic media is used to provide evidence in significant employment issues like sexual harassment, disability claims, insubordination, and posted material that would call into question the judgment of an employee.

With the increased use of social media, and the increasing reliance on the use of social media as evidence, the question is whether existing rules for evidence will be the same or different for SMS. It is a relatively new area for the courts, It is fairly well-established that the basic rules of evidence still apply. Several key decisions by the New York courts provide guidance on the discovery of social media. The courts acknowledge that social media is constantly evolving and that the rules of discovery of social media are somewhat unclear, however, the courts are generally in agreement over the following:

Social Media is Discoverable

Magistrate Judge Marilyn D. Go noted in a recent case that, “although the law regarding the scope of discovery of electronically stored information (“ESI”) is still unsettled, there is no dispute that social media information may be a source of relevant information that is discoverable.”²³¹ Just because the information is contained in electronic media is not a bar to its discovery. Other cases have echoed that sentiment. “The fact that [SMS data] exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.”²³² That same court characterized social media as an “All about me” folder that is voluntarily shared with other people.²³³ The quote indicates that the court views social media not as a private site, but a vehicle for sharing information which seems to diminish the defense of privacy against discovery.

The principles that were articulated in the New York Courts have extended to other jurisdictions. For example, in *Tompkins v. Detroit Metropolitan Airport*, the court found that

²²⁹ Jackson v. Paula Deen, Case No. CV412-139, (S.D. Georgia), SAVANNAH DIVISION
2013 U.S. Dist. LEXIS 65814, May 8, 2013.

²³⁰ *Id.* at *60.

²³¹ Reid v. Ingerman Smith LLP, , 2012 U.S. Dist. LEXIS 182439 at *2 (E.D.N.Y. Dec. 27, 2012)

²³² EEOC v. Original Honeybaked Ham Co. of Ga., 2012 WL 5430974, at *1 (D. Colo. Nov. 7, 2012).

²³³ *Id.*

defendant must make a sufficient predicate showing that the private Facebook material sought in discovery is reasonably calculated to lead to the discovery of admissible evidence.²³⁴ In *Offenback v. L.M. Bowman, Inc.*, the court granted a defense request for an in-camera review of plaintiff's private Facebook page to determine whether or not the content was responsive to the defendant's discovery requests.²³⁵ Finally in *State of Connecticut v. Eleck*, Facebook postings were not allowed to be used to impeach prosecution witness, stating that the postings had not been properly authenticated as being posted by witness, even though they originated from witness's Facebook account.²³⁶

Discovery of Social Media Cannot Be a "Fishing Expedition"

Even though courts have determined that social media information is discoverable, they are equally in agreement that discovery of social media is no excuse to conduct a fishing expedition for evidence. There is general consensus that social media is never to be used to try to dredge up evidence in a haphazard manner. For example, a broad request to obtain a user's password so the attorneys can view the SMS will not be granted without some sort of specific reference to the specifics of the material being sought and whether the evidence sought is probative and related to the issue at hand.²³⁷ The party who seeks discovery of social media must be able to point to facts that would indicate the probative nature of the social media data.²³⁸ Therefore, the party seeking the information must have some way other of convincing the court that the information on the social media site will be probative in order to gain access to the information on a social media site rather than being granted open access.

Exceptions to the "No Fishing Rule"

Although a party cannot make a broad request for discovery of social media in the hopes that they will find something to support their position, the courts have made one consistent exception – a claim of loss of enjoyment of life.²³⁹ In one case, the plaintiff was in a motor accident that caused her to have constant pain and lowered her quality of life.²⁴⁰ In that case, the court ordered the plaintiff to provide authorization information to the defense so that they could access her Facebook account. Other courts have followed suit and ordered discovery in loss of enjoyment claims,²⁴¹ but this represents only a minority of cases.²⁴²

Social Media Must Be Probative and Relevant to the Case at Hand

The Rules of Civil Procedure require that in order for information to be discoverable, it must be relevant and probative. There are several ways that the parties can demonstrate that the

²³⁴ *Tompkins v. Detroit Metropolitan Airport*, 2012 WL 179320 (E.D. Mich. Jan. 18, 2012).

²³⁵ *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371 (M.D. Pa. June 22, 2011).

²³⁶ *State of Connecticut v. Eleck*, 23 A.3d 818 (Conn. App. 2011).

²³⁷ See *Fawcett v. Altieri*, 960 N.Y.S.2d 592, 597-98 (Sup. Ct. Richmond County 2013) ("Fawcett"); *Winchell v. Lopiccio*, 38 Misc. 3d 458 (Sup. Ct. Orange County 2012); *Kregg v. Maldonado*, 98 A.D.3d 1289 (2d Dep't 2012)

²³⁸ *Kregg v. Maldonado*, 98 A.D.3d 1289 (2d Dep't 2012)

²³⁹ *Walter v. Walch*, 88 A.D.3d 872 at *3 (2d Dep't 2011)

²⁴⁰ *Id.* at *4.

²⁴¹ *Id.* See also *Cuomo*, at 3 (ordering plaintiff, who claimed that he was unable to play sports, dance or do other activities after knee surgery, to provide defendants with an authorization for access to his Facebook account).

²⁴² See, e.g., *Bianco*, at *1; *Reid*, at *2; *Winchell*, at 421-25; *Kregg*, at 1290; *Loporcaro v. City of New York*, 2012 WL 1231021, at *8 (Sup. Ct. Richmond County Apr. 9, 2012). See also *AllianceBernstein L.P. v. Atha*, 100 A.D.3d 499, 500 (1st Dep't 2012) (in-camera review of iPhone).

social media will yield probative data: Typically, parties can establish such a factual predicate by (i) showing that the opposing party has already made public the type of information sought (for example, Facebook profile pictures); (ii) pointing to deposition testimony or similar evidence showing that the SMS contains relevant information; or, to a limited extent, (iii) citing a plaintiff's claim for loss of enjoyment of life.²⁴³

In *Holly Potts v. Dollar Tree Stores*, Potts filed a Title VII discrimination and Equal Pay violations case against her employer, Dollar Tree Stores based on race discrimination and a hostile environment sexual harassment claim.²⁴⁴ She asked for a declaratory judgment. Defense filed a motion to compel discovery and stated the Plaintiff had not complied with all discovery requests. In particular, Dollar Tree wanted access to Pott's emails and Facebook materials in order to get "relevant" information regarding her claims, including the computer as well.²⁴⁵

Ms. Potts stated that surrendering the computer would be too burdensome since she had produced various emails between herself and other Dollar Tree representatives. She also asserted that she should not have to provide broad access to her Facebook account. Pott's claimed that her refusal to turn over the requested social media materials has been held by other courts to be allowed only where "the defendant makes a threshold showing that publicly available information on [Facebook] undermines the Plaintiff's claims."²⁴⁶ Plaintiff argues that the Defendant fails to make this requisite threshold showing because the contents of Plaintiff's public Facebook page do not contain any information that undermines her claim against the Defendant.²⁴⁷

The court relied on Rule 26(b)(1) to guide their decision. Relevant discovery has been "construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issues that is or may be in the case."²⁴⁸ A party may seek any information that is not privileged and is relevant to his claims or defenses.²⁴⁹ For discovery purposes, relevant means information that is probative on a party's claim or defense and information that the Court determines could "lead to the discovery of admissible evidence."²⁵⁰

²⁴³ See, e.g., *Glazer v. Fireman's Fund Ins. Co.*, 2012 WL 1197167 (S.D.N.Y. Apr. 5, 2012) ("Glazer"); *Richards v. Hertz Corp.*, 100 A.D.3d 728 (2d Dep't 2012) ("Richards"); *Bianco v. North Fork Bancorporation Inc.*, 2012 WL 5199007 (Sup. Ct. N.Y. County Oct. 10, 2012) ("Bianco"); *Walter v. Walch*, 88 A.D.3d 872 (2d Dep't 2011) ("Walter"); *Winchell*; *Heins v. Vanbourgondien*, Slip Op. (Sup. Ct. Suffolk County Sep. 25, 2012) ("Heins"); *Abizeid v. Turner Constr. Co.*, No. 23538/10 (Sup. Ct. Nassau County Sep. 5, 2012) ("Abizeid").

²⁴⁴ *Holly Potts v. Dollar Tree Stores, Inc.*, 2013 U.S. Dist. LEXIS 38795; 117 Fair Empl. Prac. Cas. (BNA) 1352. March 20, 2013

²⁴⁵ *Id.* at *4.

²⁴⁶ *Id.* citing *Thompson v. Autoliv ASP, Inc.*, 2012 U.S. Dist. LEXIS 85143, 2012 WL 2342928, *4 (D. Nev. June 20, 2012).

²⁴⁷ *Id.* at *5.

²⁴⁸ *Id.* at *5- *6 quoting *Oppenheimer Fund Inc. v. Sanders*, 437 U.S. 340, 351, 98 S. Ct. 2380, 57 L. Ed. 2d 253 (1978). A party may seek any information that is not privileged and is relevant to his claims or defenses. Fed. R. Civ. P. 26(b)(1). For discovery purposes, relevant means information that is probative on a party's claim or defense and information that the Court determines could "lead to the discovery of admissible evidence." Fed. R. Civ. P. 26(b)(1). Yet, "[t]he desire to allow broad discovery is not without limits and the trial court is given wide discretion in balancing the needs and rights of both plaintiff and defendant." *Surles v. Greyhound Lines, Inc.*, 474 F.3d 288, 305 (6th Cir.2007) (quoting *Scales v. J.C. Bradford*, 925 F.2d 901, 906 (6th Cir.1991)).

²⁴⁹ *Id.* at *6 quoting Fed. R. Civ. P. 26(b)(1).

²⁵⁰ *Id.*

Yet, the “desire to allow broad discovery is not without limits and the trial court is given wide discretion in balancing the needs and rights of both plaintiff and defendant.”²⁵¹

The court commented that the Sixth Circuit had not made any definitive ruling regarding the discovery of information on Facebook. However, it pointed to the rulings in other courts:

[M]aterial posted on a ‘private’ Facebook page, that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy. Nevertheless, the Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public view. Rather, consistent with Rule 26(b) . . . [and decisional law] . . . there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence. Otherwise, the Defendant would be allowed to engaged in the proverbial fishing expedition, in the hope that there might be something of relevance in Plaintiff’s Facebook account.²⁵²

The court concluded that the defense had not shown sufficient evidence that the Facebook account would contain any relevant information that would or should lead to the discovery of her private Facebook account. In addition, since Potts produced her “day planner, documentation of ‘write-ups’ and ‘store visits,’ emails between Plaintiff, Trowery and other employees at Dollar Tree, as well as all relevant information stored on her computer. Plaintiff asserts that she no longer has possesses any photographs of the Dollar Tree store.”²⁵³ Thus, the Court concludes that Defendant has not made the requisite showing for full access to Plaintiff’s private Facebook or other social media pages.²⁵⁴ In other words, there was nothing on the public areas of Pott’s Facebook account or in her emails that would warrant further investigation into her emails or social media.

The standard of discovery for social media material was more clearly articulated in the case of the *EEOC v. The Original Honeybaked Ham Company*, a case involving Title VII sexual harassment and retaliation. In this case, the EEOC represented a class of female employees who worked at the Original Honeybaked Ham Company (HBH) in the sexual harassment suit. HBH filed a motion to compel discovery of the plaintiffs’ social media pages to assess their emotional and financial damages.²⁵⁵ As the judge stated:

“[I]n certain respects justifiable) intrusion into the class member's semi-private lives, and because the whole area of social media presents thorny and novel issues with which courts are only now coming to grips, I will not determine this motion or any sanctions

²⁵¹ *Id.* quoting *Surles v. Greyhound Lines, Inc.*, 474 F.3d 288, 305 (6th Cir.2007) (quoting *Scales v. J.C. Bradford*, 925 F.2d 901, 906 (6th Cir.1991)).

²⁵² *Id.* at *6 - *7 quoting *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012); see also *McCann v. Harleystown Ins. Co. of N.Y.*, 78 A.D.3d 1524, 1525, 910 N.Y.S.2d 614 (N.Y. App. Div. 2010) (holding that Defendant failed to establish a factual predicate with respect to the relevancy of the evidence on the Facebook page and that Defendant essentially sought permission to conduct a fishing expedition).

²⁵³ *Id.* at *7 - *8.

²⁵⁴ *Id.* at *8.

²⁵⁵ *Equal Employment Opportunity Commission, v. The Original Honeybaked Ham Company of Georgia, Inc.*, Civil Action No. 11-cv-02560-MSK-MEH United States District Court for the District of Colorado 2012 U.S. Dist. LEXIS 160285; 116 Fair Empl. Prac. Cas. (BNA) 743; 96 Empl. Prac. Dec. (CCH) P44,675 November 7, 2012.

based on what should or should not have been provided prior to this Order, nor will I apportion fault in failing to produce documents or information prior to this Order.”²⁵⁶

Furthermore, the judge stated:

Many of the class members have utilized electronic media to communicate -- with one another or with their respective insider groups -- information about their employment with/separation from Defendant HBH, this lawsuit, their then-contemporaneous emotional state, and other topics and content that Defendant contends may be admissible in this action. As a general matter, I view this content logically as though each class member had a file folder titled "Everything About Me," which they have voluntarily shared with others. If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.²⁵⁷

The judge stated that the Defense had already shown the relevance of social media data since it was able to obtain some material from the class members' social media sites.²⁵⁸ She ordered the following:

Given the fact that Defendant has already obtained one affected former employee's Facebook pages, and that those pages contain a significant variety of relevant information, and further, that other employees posted relevant comments on this Facebook account, I agree that each class member's social media content should be produced, albeit *in camera* in the first instance. I do not believe this is the proverbial fishing expedition; these waters have already been tested, and they show that further effort will likely be fruitful. However, I am appreciative of privacy concerns and am not sold on all of Defendant's alleged areas of relevant information, particularly regarding expressions of positive attitude about this or that. Therefore, I will establish a process designed to gather only discoverable information. To accomplish this, I will utilize a forensic expert as a special master as needed. Plaintiff-Intervenor and the class members shall provide the following directly and confidentially to the special master:

1. Any cell phone used to send or receive text messages from January 1, 2009 to the present;
2. All necessary information to access any social media websites used by such person for the time period January 1, 2009 to present;

²⁵⁶ *Id.* at *3.

²⁵⁷ *Id.* at *3 - *4.

²⁵⁸ *Id.* at *4 - *5. The court reviewed this evidence which contained discoverable information. Defendant has shown, for example, that Plaintiff-Intervenor Cabrera posted on her Facebook account statements that discuss her financial expectations in this lawsuit²; a photograph of herself wearing a shirt with the word "CUNT" in large letters written across the front (a term that she alleges was used pejoratively against her, also alleging that such use offended her)³; musings about her emotional state in having lost a beloved pet as well as having suffered a broken relationship⁴; other writings addressing her positive outlook on how her life was post-termination⁵; her self-described sexual aggressiveness⁶; statements about actions she engaged in as a supervisor with Defendant (including terminating a woman who is a class member in this case); sexually amorous communications with other class members⁷; her post-termination employment and income opportunities and financial condition; and other information.”

3. All necessary information to access any email account or web blog or similar/related electronically accessed internet or remote location used for communicating with others or posting communications or pictures, during the time period January 1, 2009 to present.²⁵⁹

The judge ordered the parties to collaborate and come up with a questionnaire for all members of the class as to the material that they had on Facebook. If the response yielded relevant information, then the court could compel the parties to produce the Facebook evidence. If there were any dispute about the relevance of that information, the dispute would be resolved by the judge's in-camera review of the disputed material.²⁶⁰ The judge saw this as a viable compromise between the privacy interests of the plaintiffs and the need to discover relevant information for the case.

Establishing the Evidentiary Predicate for Discovery of Social Media

There are several ways that the parties can demonstrate that the social media will yield probative data: Typically, parties can establish such a factual predicate by (i) showing that the opposing party has already made public the type of information sought (for example, Facebook profile pictures); (ii) pointing to deposition testimony or similar evidence showing that the SMS contains relevant information; or, to a limited extent, (iii) citing a plaintiff's claim for loss of enjoyment of life.²⁶¹

Using Depositions to Establish the Evidentiary Predicate

This brings up an issue: what are the discovery rules for material contained in private areas of social media versus those areas on view to the public. Fewer and fewer people are posting information on public areas. So, some legal analysts have stated that if this is the case, attorneys can look to depositions to establish grounds for social media discovery requests.²⁶² So, if a plaintiff makes a reference to his or her Facebook account while being deposed, the door is opened for the court to order discovery of the social media. For example, in *Cuomo v. 53rd & 2nd Assocs., LLC*, the plaintiff had referenced his Facebook account during a deposition and the court ordered the discovery of the information contained in his account.²⁶³

In *Glazer v. Fireman's Fund Ins. Co.*, the plaintiff sued her employer on the basis of race discrimination and religious discrimination.²⁶⁴ The defense attorneys requested transcripts of her chats with a psychic from LivePerson (an internet chat site). "The defendants were able to produce emails (which the plaintiff had sent to herself) containing excerpts of certain chats concerning the plaintiff's work performance, relationships with co-workers, treatment by the defendants, and personal beliefs about African-Americans. Although the court did not compel LivePerson to produce the transcripts, it did order the plaintiff to open a new LivePerson account

²⁵⁹ *Id.* at *7 - *8.

²⁶⁰ *Id.* at *8.

²⁶¹ See, e.g., *Glazer v. Fireman's Fund Ins. Co.*, 2012 WL 1197167 (S.D.N.Y. Apr. 5, 2012) ("Glazer"); *Richards v. Hertz Corp.*, 100 A.D.3d 728 (2d Dep't 2012) ("Richards"); *Bianco v. North Fork Bancorporation Inc.*, 2012 WL 5199007 (Sup. Ct. N.Y. County Oct. 10, 2012) ("Bianco"); *Walter v. Walch*, 88 A.D.3d 872 (2d Dep't 2011) ("Walter"); *Winchell*; *Heins v. Vanbourgonien, Slip Op.* (Sup. Ct. Suffolk County Sep. 25, 2012) ("Heins"); *Abizeid v. Turner Constr. Co.*, No. 23538/10 (Sup. Ct. Nassau County Sep. 5, 2012) ("Abizeid").

²⁶² Schulman, B.M., Ettari, S.V., and Neunder, L. *New York Courts Address the Electronic Discovery of Social Media*, THE METROPOLITAN CORPORATE COUNSEL, page 17, May 2013.

²⁶³ *Cuomo v. 53rd & 2nd Assocs., LLC*, No. 111329/10 (Sup. Ct. N.Y. County Aug. 27, 2012).

²⁶⁴ *Glazer v. Fireman's Fund Ins. Co.*, 2012 WL 1197167 (S.D.N.Y. Apr. 5, 2012)

so that she could access her old chats and produce all LivePerson chats to the defendants.”²⁶⁵ The chats contained information about her feelings towards African-Americans, her work performance, her relationships with others and the defendant’s treatment of her.²⁶⁶ In the end, the court did not compel LivePerson to produce the transcripts. It required the plaintiff to open a new LivePerson account and then had her retrieve all of the LivePerson chats.²⁶⁷

If the party can demonstrate that the SMS data is probative and relevant, the next concern is to prove that the SMS data information requested has actually been posted by the user in question. In other words, the SMS data must be authenticated.

Authentication of SMS evidence

Websites themselves are not self-authenticating.²⁶⁸ In order to satisfy the requirement that evidence must be trustworthy, Rule 901(a) states that there must be a showing of evidence to prove the evidence is authentic and is what it is purported to be.²⁶⁹ In *United States v. Safavian*,²⁷⁰ the court stated:

The question for the Court under Rule 901 is whether the proponent of the evidence has "offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is." The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so²⁷¹

Three questions must be answered in order to properly authenticate SMS evidence, "(1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?"²⁷² It is critical to answer these three questions and also to consider:

The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question?²⁷³

²⁶⁵ Schulman, pg 17.

²⁶⁶ Schulman citing to Glazer pg **1, 12-13.

²⁶⁷ *Id.*

²⁶⁸ *St. Luke's Cataract & Laser Institute P.A. v. Sanderson*, 2006 WL 1320242, at *1.

²⁶⁹ FED. R. EVID. 901(a)

²⁷⁰ *United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006).

²⁷¹ *Id.* at 38.

²⁷² Jonathan D. Frieden & Leigh M. Murray, The Admissibility of Electronic Evidence Under the Federal Rules of Evidence, 17 RICH. J.L. & TECH. 5, 11 (2010) (quoting Keiko L. Sugisaka, Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual?, 35 WM. MITCHELL L. REV. 1453, 1459 (2009)).

²⁷³ Diaz, Adam Alexander, "Getting Information off the Internet Is like Taking a Drink from a Fire Hydrant" --The Murky Area of Authenticating Website Screenshots in the Courtroom, 37 Am. J. Trial Advoc. 65, (Spring 2013) quoting *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 55-56 (D. Md. 2007) (quoting 5 STEVEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL § 901.02[12] (9th ed. 2006)).

To complicate matters, there are various types of possible evidentiary material from SMS: (1) personal messages sent via social networking websites; (2) postings on an individual account holder's web pages; (3) photographs posted on an individual's account or web page; and (4) "tags," in which one account-holder lists another individual's name to indicate that that person is in a photograph, at an event, or simply has something to do with a comment.²⁷⁴ Each presents unique issues regarding authentication and presents different privacy concerns.

DIFFERENT TYPES OF INFORMATION ON SMS

SMS Messaging

Facebook and other social media sites allow for messaging. In general, the user must log into their account and can send messages to a designated individual or a group of individuals. It is not surprising the courts have utilized the evidentiary model for email.²⁷⁵ In fact:

In its survey of ESI authentication across the federal system, the District Court of Maryland noted that "[t]he most frequent ways to authenticate e-mail evidence are 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), [and] 901(b)(4) (distinctive characteristics, including circumstantial evidence)." Indeed, all three of these methods are used to authenticate internet postings in general.²⁷⁶

The first method, known as the E-Mail Parallel Approach, treats messaging as email and is probably the standard that is the easiest to authenticate. All that seems to be required is a showing that the message came from the poster's account.²⁷⁷ Even though it is always a possibility that someone else sent a message from the user's account, some courts have found that this is not a bar to authentication, but is a matter for the jury to decide.²⁷⁸

The second approach is known as the Corroboration Approach. In this approach, the court will use circumstantial evidence to verify that messages that are sent from SMS sites are actually authored by the sender in question.²⁷⁹ For example, when emails are authenticated, many times a court will require evidence of knowledge of the content of the email that would only be known to the sender and/or the recipient.²⁸⁰ For example, in one rape case where MySpace messages were being introduced, the court considered those messages to be properly authenticated if: "(1) a witness recognized the e-mail address as belonging to the defendant; (2) the e-mails discussed information only the victim, defendant, and a few other people knew; and (3) the e-mails were written in a way the defendant was known to communicate".²⁸¹

²⁷⁴ Mehlman, Julia, Facebook and MySpace in the Courtroom: Authentication of Social Networking Websites, 8 Crim. L. Brief 9, (Fall, 2012).

²⁷⁵ *Id.*, at 12.

²⁷⁶ *Id.*, quoting Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, at 555-6 (D. Md. 2007).

²⁷⁷ *Id.*, at 12.

²⁷⁸ *Id.*, at 12-13. Mehlman uses the case of *People v. Clevestine*, 891 N.Y.S.2d 511, 513 (N.Y. App. Div. 2009) which was a rape case that made use of MySpace messaging as evidence.

²⁷⁹ *Id.*, at 13.

²⁸⁰ *Id.*

²⁸¹ *Id.*, The author cites to the case of *Manuel v. State*, 357 S.W.3d 66, 75 (Tex. Ct. App. 2011) which stated that MySpace and Facebook messages can be used in the same way as email messaging based on "[a]pppearance,

The third approach, the Security Approach, authenticates SMS messaging by revealing the security and privacy procedures of the SMS site.²⁸² If the SMS has very strict access rules and maintains the privacy of its members, it is a fair conclusion that the information posted is more likely to have been authored and posted by the user.

Examples of SMS messaging as evidence

Another significant case regarding the discoverability of social media and texting information is found in the *City of Ontario v. Quon*, where pager texts and Facebook information was used to see if police officers had misused the pagers provided by the police department.

City of Ontario, California v. Quon.²⁸³ The City of Ontario had given their police officers alphanumeric pagers. The police department had placed limits on how many alphanumeric characters the officers were allotted. The officers would be charged for any messages that went over the allotted quota. Quon, along with several other officers, went over the allotment for several months. The City decided to determine the reasons behind the overages. Specifically, they were trying to determine whether the limit was too low and officers had to pay for work-related pages or whether the overages were due to personal messages.²⁸⁴ The provider gave Quon's police chief transcripts of Quon's messages. Most of them were not work-related and some of them were sexually explicit.²⁸⁵ The matter was turned over to the Internal Affairs department that concluded that few of Quon's on duty messages were related to work. Quon was disciplined for violating the Ontario Police Departments rules.²⁸⁶

As a result, Quon and some of the other officers that exchanged messages with Quon, brought a suit against the City had violated their Fourth Amendment Rights and had committed violations of the Stored Communications Act (SCA) for obtaining and reviewing the transcripts and against the provider for providing the transcripts. The District Court refused to grant summary judgment to the city stating that a determination must be made to assess whether Quon had a reasonable expectation of privacy. A key piece of the analysis is whether the Chief of Police conducted the investigation for the improper purpose of determining how Quon used the pager on his off time or for the proper purpose of seeing whether officers were being charged for work related overages. The jurors concluded the Chief of police did conduct his investigation for a legitimate purpose. The District court then granted the City summary judgment that the search did not constitute a violation of the Fourth Amendment given that it was a legitimate search. The Ninth Circuit reversed. While the Ninth Circuit agreed that the search was done for legitimate purposes, the same purpose could be achieved by using less intrusive means.²⁸⁷

Can a search of social media violate the Fourth Amendment? The Supreme Court granted certiorari, for Quon and found that the Ninth Circuit had erred and referred back to the analysis that was put forward in *Ortega v. O'Connor*,²⁸⁸ where the Justices in that case

contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with circumstances." The Manuel case relied on *Massimo v. State*, 144 S.W.3d 210, 215-17 (Tex. Crim. App. 2004)

²⁸² *Id.* at 14.

²⁸³ *City of Ontario, California v. Jeff Quon*, 130 S. Ct. 2619 (2010)

²⁸⁴ *Id.* at 2621.

²⁸⁵ *Id.*

²⁸⁶ *Id.*

²⁸⁷ *Id.*

²⁸⁸ *Ortega v. O'Connor*, 480 U.S. 709, (1987).

developed the standard for analyzing whether a governmental employer had improperly breached the Fourth Amendment rights of an employee. The Justices had developed a two-part proof:

First, because "some [government] offices may be so open . . . that no expectation of privacy is reasonable," a court must consider "[t]he operational realities of the workplace" to determine if an employee's constitutional rights are implicated.²⁸⁹ Second, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."²⁹⁰

The Court refused to definitively state whether Quon had an expectation of privacy since the Court recognized that the state of technology is changing at such a rapid rate that any pronouncements of expectations of privacy would quickly become outdated. The Court stated that they would assume that Quon had an expectation of privacy and on that basis, stated that the warrantless investigation of the pager messages that was spearheaded by the chief of police was a reasonable search since it was for legitimate work-related purposes. Given the fact that only a few of the many pager messages were used to investigate Quon's pager activity and given the fact that any off-duty messages were redacted from the transcript, the Court decided that the search was reasonable and Quon's limited expectation of privacy was not violated.²⁹¹

Unlike their public sector counterparts, private sector employees do not have many rights when it comes to expectation of privacy. Even private employees have the belief that they have a "right to privacy" under the Constitution along with protections against illegal search and seizure. Therefore, discoverability of social media for private sector firms is not focused on whether the employee has a right to privacy (and many courts would say expectations of privacy on social media may not shield an employee from having to turn over evidence contained on a social media site. However, the courts are beginning to articulate the litmus-tests regarding whether social media material will be discoverable. Case law will shape the discovery guidelines since most federal laws up to this point present a "piecemeal" approach to regulating electronic monitoring in private employment.²⁹²

SMS Postings as Evidence

Postings on SMS are distinct from messaging from sites such as Facebook and MySpace. For example, on Facebook, each user has their own "wall" on which can be posted comments, pictures, and other material. The postings are visible to whoever has the permission to view the posts – typically friends and family of the user. But in addition to posts by the account holder, other users can post on the account holder's website and it is for this reason that the courts treat postings differently than with emails. Rather than comparing postings to email, the courts have found postings to be more similar to other types of web postings and as such, require the same

²⁸⁹ *Id.*

²⁹⁰ *Id.* at 725-726.

²⁹¹ *Id.*

²⁹² Ciocchetti, Corey A. *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 ACADEMY OF LEGAL STUDIES IN BUSINESS AMERICAN BUSINESS LAW JOURNAL, 285, 291 Summer, 2011. ("Employers are restricted only in rare situations where their employees possess a reasonable expectation of privacy in the workplace or where they have been careless enough to violate flimsy state laws, federal laws, or the common law tort of intrusion upon seclusion.")

kind of authentication procedures.²⁹³ Postings present more authentication issues since anyone who may hack into a person's profile may post information and appear to look like the rightful account holder. Furthermore, anyone who is the "friend" of the original account holder may post on the site and there is no direct way of knowing whether the poster is that person or not. There have been instances of hackers gaining control of someone's account and sending messages and well as posts to other users with the recipient unable to tell whether the sender is a hacker or the account holder.

Rubino v. City of New York. A recent example of social media discovery in the public sector is the experience of a New York teacher who was dismissed because of what she had posted on her Facebook account. Christine Rubino was a tenured teacher in the New York Public School system. On June 22, 2010, a public school student had drowned while on a field trip to a beach. The day after the incident, Ms. Rubino posted on her Facebook page: "After today, I am thinking the beach sounds like a wonderful idea for my 5th graders! I HATE THEIR GUTS! They are the devils (sic) spawn!" One of her Facebook friends then posted, "oh you would let little Kwame float away!" to which petitioner responded, "Yes, I wld (sic) not throw a life jacket in for a million!!"²⁹⁴

One of her Facebook friends (who happened to be a colleague who worked with her at the same school) contacted the assistant principal to express her concern about the propriety of the posting. On June 24, 2010, the assistant principal showed the postings to the principal, and upon her instruction, contacted the Special Commissioner of Investigation for the New York City School District (SCI), which initiated an investigation.²⁹⁵ The investigator was able to view the postings since her Facebook account was linked and recommended in his final report that Rubino should be terminated.²⁹⁶

Interestingly enough, when she was confronted with the report, Rubino claimed she didn't know anything about it and named a friend who had access to her account, suggesting that her friend might have made the postings. Initially, when the friend was confronted and asked about this, she said she did make the postings but then recanted her story a few days later when the investigator told her that he didn't believe her and warned her that she could be incarcerated for perjury. Her friend claimed that Rubino had convinced her to take the blame since Rubino was worried about losing her job.²⁹⁷ The SCI reporter summarized the interview and entered a new report in which he recommended Rubino's termination.²⁹⁸

The Department of Education made its own charges against Rubino and cited that her postings on Facebook which included the original statement and the statement, "'after today, I'm thinking the beach sounds like a wonderful idea for my 5th graders! I HATE THEIR GUTS! They are all the devils (sic) spawn!"²⁹⁹ Rubino was also charged with having her friend take the blame for the postings. At the ensuing hearing, Rubino admitted to the postings and apologized

²⁹³ *Id.*, at 15-16.

²⁹⁴ *Rubino v. City of New York*, 34 Misc. 3d 1220A; 2012 N.Y. Misc. LEXIS 468; 2012 NY Slip Op 50189U, Supreme Court of New York, February 1, 2012. at 2.

²⁹⁵ *Id.*

²⁹⁶ *Id.*

²⁹⁷ *Rubino* at 3.

²⁹⁸ *Id.*

²⁹⁹ *Id.* at 4.

saying that she had taken the postings down after two days and if she could take back what she did she would.³⁰⁰ She repeatedly denied asking her friend to take the blame for the postings.³⁰¹ The hearing officer recommended that she be terminated underscoring the fact that she was acting as a teacher in a public forum and that she persistently blamed her friend for the postings thus obstructing the investigation.³⁰² Her actions of taking down the postings did not remove the harm that they did since her postings would leave a “lasting footprint” on the Internet since the material had been seen and disseminated by others.³⁰³

Rubino asserted that the hearing officer’s remedy was harshly disproportionate to her offense since she had an unblemished record for fifteen years. She also claimed that her Constitutional First Amendment rights were violated however, the court declined to consider this matter since she was acting in her professional capacity as a teacher and because of the hearing officer’s conclusion that Facebook postings do not constitute protected speech under the Constitution.³⁰⁴ The court declined to consider the issues of violation of public policy as well, but did conclude that the punishment of termination was not in line with the offense of the postings since the postings neither were intended to harm the students nor did it harm the students in fact.³⁰⁵ The court ordered the Rubino’s termination to be vacated and remanded the case back to the Board for a more appropriate penalty. What is interesting to note is the court’s view of FaCebook postings:

“Indeed, with Facebook, as with social media in general, one may express oneself as freely and rapidly as when conversing on the telephone with a friend. Thus, even though petitioner should have known that her postings could become public more easily than if she had uttered them during a telephone call or over dinner, given the illusion that Facebook postings reach only Facebook friends and the fleeting nature of social media, her expectation that only her friends, all of whom are adults, would see the postings is not only apparent, but reasonable.”³⁰⁶

Many other courts have concluded that statements posted on the Internet would rarely invoke an expectation of privacy given the very unsecure nature of the Internet itself. However, the *Rubino* court felt that some expectation of privacy should be allowed, yet, the material posted on Facebook was discoverable and allowed as evidence.

Photographs and SMS

Social media sites like Facebook allow users to post photographs in several ways. The first example is the “profile picture” of the user. The user can use any type of photo – of someone famous, a work of art, a symbol or an actual picture of himself or herself. The second example is the photo albums of the user. The user can post photographs that the user took or post other photos that other people have posted and the user copies it over to his or her photo albums. The photo albums are a bit more public than messaging and anyone having permission to see the user’s public profile. Furthermore, photos can be shared and copied amongst users.

³⁰⁰ *Id.* at 5.

³⁰¹ *Id.* at 6.

³⁰² *Id.* at 8-9.

³⁰³ *Id.*

³⁰⁴ *Id.* at 12.

³⁰⁵ *Id.*

³⁰⁶ *Id.* at 17-19.

Not only can photographs be easily shared, but there is a concern that photos can be easily manipulated. Digital photography and computer software makes it very easy to alter photographs.³⁰⁷ So, any photograph posted on a SMS must be authenticated "by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately describes [the scene],"³⁰⁸ and that "the court must also find that a reasonable juror could conclude that the photograph has not been altered in any impermissible way".³⁰⁹ Cases involving loss of enjoyment make heavy use of SMS photographs to demonstrate whether someone's physical condition is genuine or a fraud.

Social Media in Cases Involving Loss of Enjoyment

There are some cases in which the individuals will claim that they are physically unable to perform some sort of work or are severely limited in their performance. Social media can provide invaluable information to obtain photographic evidence that the party is not as disabled as they claim to be. For example, in *Abizeid v. Turner Constr. Co.*, the plaintiff had a slip and fall in the stairway of a parking garage. She claimed that the injuries she sustained were permanent, constant and debilitating. Unfortunately for her, she had posted pictures of herself at various activities such as being a bridesmaid and vacation photos of her "off-roading" which is an activity she would not have been able to do if she actually suffered the injuries she claimed. The pictures were posted in a public area of her Facebook page and the defense was able to use those pictures to contradict her claim.³¹⁰ In *Richards v. Hertz Corp.*, the plaintiff claimed she had sustained injuries from an auto accident that diminished her ability to play sports. The defense used pictures of the plaintiff skiing that were posted in the public area of her Facebook account.³¹¹ Because the plaintiff had posted these pictures in a public area and the fact that these pictures were directly relevant and probative of the extent of the plaintiff's injuries, the court allowed further discovery of the Facebook account. What is very interesting is that in both *Abizeid* and *Richards*, the court did not order the plaintiffs to disclose their Facebook passwords to opposing council. In order to protect the privacy of the user's Facebook account, the court conducted an in-camera review of the Facebook material to determine whether there was any relevant material in the private areas of the accounts. This was done to ensure that the court did not breach the privacy of the plaintiffs and did not overreach in the effort to discover relevant social media information.

Reasons for Employer Intrusions Into Social Media

Employers' use of social media and other electronic media is not uncommon. For many years now, employers have relied on electronic monitoring to uncover theft, sexual and racial harassment, and to check on the activities of their employees that may interfere with the employees' productivity such as web surfing and emailing friends. More serious concerns arise when electronic media is used to provide evidence in significant employment issues like sexual

³⁰⁷ Mehlman, at 18.

³⁰⁸ *Id.*, at 18 quoting *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 561 (D. Md. 2007).

³⁰⁹ *Id.*, See also *People v. Beckley*, 110 Cal. Rptr. 3d 362, 363 (Ct. App. 2010); and *People v. Lenihan*, 911 N.Y.S.2d 588, 592 (N.Y. Sup. Ct. 2010) (the court indicated that since it was possible to alter a digital photograph, it could not be authenticated).

³¹⁰ *Abizeid v. Turner Constr. Co.*, No. 23538/10 at 2(Sup. Ct. Nassau County Sep. 5, 2012)

³¹¹ *Richards v. Hertz Corp.*, 100 A.D.3d 728 (2d Dep't 2012).

harassment, disability claims, insubordination, and posted material that would call into question the judgment of an employee.

The issue is whether discovery of such material can take place in a medium that is thought to be private. Concerns may vary depending upon whether the employer is a public or private employer. Public sector employers have the additional concern about whether or not discovery requests will violate an employee's Constitutional rights with respect to expectation of privacy of social media.

The standard of discovery for social media material was more clearly articulated in the case of the *EEOC v. The Original Honeybaked Ham Company*, a case involving Title VII sexual harassment and retaliation. In this case, the EEOC represented a class of female employees who worked at the Original Honeybaked Ham Company (HBH) in the sexual harassment suit. HBH filed a motion to compel discovery of the plaintiffs' social media pages to assess their emotional and financial damages.³¹² As the judge stated:

“[I]n certain respects justifiable) intrusion into the class member's semi-private lives, and because the whole area of social media presents thorny and novel issues with which courts are only now coming to grips, I will not determine this motion or any sanctions based on what should or should not have been provided prior to this Order, nor will I apportion fault in failing to produce documents or information prior to this Order.”³¹³

Furthermore, the judge stated:

Many of the class members have utilized electronic media to communicate -- with one another or with their respective insider groups -- information about their employment with/separation from Defendant HBH, this lawsuit, their then-contemporaneous emotional state, and other topics and content that Defendant contends may be admissible in this action. As a general matter, I view this content logically as though each class member had a file folder titled "Everything About Me," which they have voluntarily shared with others. If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.³¹⁴

The judge stated that the Defense had already shown the relevance of social media data since it was able to obtain some material from the class members' social media sites.³¹⁵ She ordered the following:

³¹² Equal Employment Opportunity Commission, v. The Original Honeybaked Ham Company of Georgia, Inc., Civil Action No. 11-cv-02560-MSK-MEH United States District Court for the District of Colorado 2012 U.S. Dist. LEXIS 160285; 116 Fair Empl. Prac. Cas. (BNA) 743; 96 Empl. Prac. Dec. (CCH) P44,675 November 7, 2012.

³¹³ *Id.* at *3.

³¹⁴ *Id.* at *3 - *4.

³¹⁵ *Id.* at *4 - *5. The court reviewed this evidence which contained discoverable information. Defendant has shown, for example, that Plaintiff-Intervenor Cabrera posted on her Facebook account statements that discuss her financial expectations in this lawsuit²; a photograph of herself wearing a shirt with the word "CUNT" in large letters written across the front (a term that she alleges was used pejoratively against her, also alleging that such use offended her)³; musings about her emotional state in having lost a beloved pet as well as having suffered a broken relationship⁴; other writings addressing her positive outlook on how her life was post-termination⁵; her self-described sexual aggressiveness⁶; statements about actions she engaged in as a supervisor with Defendant (including terminating a woman who is a class member in this case); sexually amorous communications with other class

Given the fact that Defendant has already obtained one affected former employee's Facebook pages, and that those pages contain a significant variety of relevant information, and further, that other employees posted relevant comments on this Facebook account, I agree that each class member's social media content should be produced, albeit *in camera* in the first instance. I do not believe this is the proverbial fishing expedition; these waters have already been tested, and they show that further effort will likely be fruitful. However, I am appreciative of privacy concerns and am not sold on all of Defendant's alleged areas of relevant information, particularly regarding expressions of positive attitude about this or that. Therefore, I will establish a process designed to gather only discoverable information. To accomplish this, I will utilize a forensic expert as a special master as needed. Plaintiff-Intervenor and the class members shall provide the following directly and confidentially to the special master:

1. Any cell phone used to send or receive text messages from January 1, 2009 to the present;
2. All necessary information to access any social media websites used by such person for the time period January 1, 2009 to present;
3. All necessary information to access any email account or web blog or similar/related electronically accessed internet or remote location used for communicating with others or posting communications or pictures, during the time period January 1, 2009 to present.³¹⁶

The judge ordered the parties to collaborate and come up with a questionnaire for all members of the class as to the material that they had on Facebook. If the response yielded relevant information, then the court could compel the parties to produce the Facebook evidence. If there were any dispute about the relevance of that information, the dispute would be resolved by the judge's in-camera review of the disputed material.³¹⁷ The judge saw this as a viable compromise between the privacy interests of the plaintiffs and the need to discover relevant information for the case.

Although the Rules of Civil Procedure require that in order for information to be discoverable, it must be relevant and probative, there are unique problems associated with social media that cause headaches for attorneys. Recent decisions from New York may very well provide some consistency in other jurisdictions as to how to properly determine whether or not social media is discoverable.

Social Media in Cases Involving Loss of Enjoyment

There are some cases in which the individuals will claim that they are physically unable to perform some sort of work or are severely limited in their performance. Social media can provide invaluable information to obtain evidence showing evidence to the contrary. For example, in *Abizeid v. Turner Constr. Co.*, the plaintiff had a slip and fall in the stairway of a parking garage. She claimed that the injuries she sustained were permanent, constant and debilitating. Unfortunately for her, she had posted pictures of herself at various activities such as being a bridesmaid and vacation photos of her "off-roading" which is an activity she would not have been able to do if she actually suffered the injuries she claimed. The pictures were posted

members⁷; her post-termination employment and income opportunities and financial condition; and other information."

³¹⁶ *Id.* at *7 - *8.

³¹⁷ *Id.* at *8.

in a public area of her Facebook page and the defense was able to use those pictures to contradict her claim.³¹⁸ In *Richards v. Hertz Corp.*, the plaintiff claimed she had sustained injuries from an auto accident that diminished her ability to play sports.

The defense used pictures of the plaintiff skiing that were posted in the public area of her Facebook account.³¹⁹ Because the plaintiff had posted these pictures in a public area and the fact that these pictures were directly relevant and probative of the extent of the plaintiff's injuries, the court allowed further discovery of the Facebook account. What is very interesting is that in both *Abizeid* and *Richards*, the court did not order the plaintiffs to disclose their Facebook passwords to the opposition so that the entirety of their account could be examined. Instead, the courts conducted an in-camera review of the Facebook material to determine whether there was any relevant material in the private areas of the accounts. This was done to ensure that the court did not breach the privacy of the plaintiffs and did not overreach in the effort to discover relevant social media information.

Social Media and Preservation of Data

Other cases have raised the concern about handling social media and the possible issues that arise regarding the preservation of the data and actions that may result in sanctions with regards to the spoliation of the material.³²⁰ While such a decision of spoliation is rare, it does happen. A recent Virginia state court decision, however, demonstrates the ramifications of poor decisions by both counsel and parties when dealing with run-of-the-mill discovery requests that have a social media element.

Allied Concrete Co., v. Lester (Va. Cir. Ct. Oct 21, 2011), was a wrongful death case stemming a collision of truck loaded with concrete with that of a passenger car containing Lester and his wife. In 2008, truck driver William Donald Sprouse pleaded guilty to charges of involuntary manslaughter for the accidental death of Jessica Lester. According to news reports, Sprouse's "truck rounded a corner on two wheels, flipped and rolled over onto Lester's car, a crushing 60,000 pounds landing where Jessica sat." Jessica Lester's husband of two years and her parents subsequently sued Allied (Sprouse's employer) and Sprouse, eventually winning a jury verdict of over \$10 million, making it reportedly one of the largest wrongful death verdicts in the state's history.³²¹

Shortly after that, there were a number of complaints from defense council regarding the conduct of the plaintiff (who was the decedent's husband) and his attorney charging the with spoliation of Lester's Facebook account. Allied's counsel had learned that there was a picture of Lester on his Facebook page where his appearance provided contrary to his own testimony that he was grieving for his deceased wife. The picture portrayed Lester in a T-shirt which said "I [heart} hot moms" and holding a beer can standing with young adults. Allied's attorneys presented the photo to the court with a discovery request for all of the Facebook postings from the time of the request.³²²

³¹⁸ *Abizeid v. Turner Constr. Co.*, No. 23538/10 at 2(Sup. Ct. Nassau County Sep. 5, 2012)

³¹⁹ *Richards v. Hertz Corp.*, 100 A.D.3d 728 (2d Dep't 2012).

³²⁰ Landon, Jana M. Is A Facebook Page Worth Your Job? E-Discovery And Spoliation In The Age Of Social Media, The Metropolitan Corporate Counsel, pg. 18, May 2012

³²¹ *Allied Concrete Co., v. Lester* (Va. Cir. Ct. Oct 21, 2011); see also *Lester v. Allied Concrete Co.*, No. 736 S.E.2d 699, 701(2013).

³²² *Id.* at 702.

When Lester's attorney, Murray, received the request he immediately instructed his assistant to email his client with instructions to clean up the Facebook page. The assistant sent the email off the next day. Murray then instructed his client to deactivate the page entirely, so that he could represent in his response to the discovery requests that he had "no page as of the date of the response." After further wrangling between the parties, the page was re-activated so that screenshots could be taken, but Lester then "cleaned up" the page consistent with the prior instructions, deleting 16 photographs and other evidence. Lester later denied during his deposition that he ever deactivated his account.³²³

Suspicious about these activities and Lester's testimony, defense counsel subpoenaed from Murray all e-mails between Murray and Lester that related to the Facebook account. Not surprisingly, Murray and Lester resisted, claiming work product and attorney-client privilege. When the court ordered Murray to produce a privilege log, he did so, but he withheld the e-mail from his assistant instructing Lester to clean up his Facebook page. Murray subsequently produced the e-mail to the judge, claiming the omission was an oversight by a paralegal.³²⁴

The court found this behavior to be aberrant and that due to "the extensive pattern of deceptive and obstructionist conduct of Murray and Lester ... most of the substantial fees and costs expended by Defendants were necessary and appropriate to address and defend against such conduct." The court also found specifically that Lester intentionally spoiled evidence.

Ultimately, the wrongful death verdict was slashed to \$4.45 million for reasons ostensibly unrelated to Lester's and Murray's conduct. Moreover, the court sanctioned Murray in the amount of \$542,000, and Lester in the amount of \$180,000, citing as primary reasons their actions relating to Lester's Facebook page.³²⁵ Murray's conduct was referred to the Virginia State Bar. Since the court's October 2011 ruling, Murray reportedly has left his position at his law firm and quit the practice of law.

Cautions regarding Discovery of Social Media

The Lester case was highly unusual, but it does bring to mind some real issues of concern that are raised with using social media materials as evidence. Joan Landon summarizes these concerns below:

1. *Don't Forget That the Rules Still Apply.* When new technology is introduced to discovery, many attorneys try to stretch the limits of discovery as far as possible. For example, when parties first began to produce documents in electronic rather than paper form, many attorneys would purposely not produce load files, searchable text, or any metadata – all things now considered to be commonplace – in order to "one-up" their opponents. Similarly, there may be a tendency to think that social media accounts provide a strategic opportunity for gamesmanship, because social media can be mercurial and capable of manipulation. Attorneys should be aware, however, that the same rules of evidence apply to social media sites as to other evidence. Accordingly, in the same way you would not instruct a client to shred files or trash a hard drive, no changes should be made to relevant or potentially responsive evidence on social media accounts once litigation is reasonably anticipated. Also, know the rules of your jurisdiction – courts are becoming increasingly savvy with e-discovery and several of them have particular

³²³ *Id.* at 703.

³²⁴ *Id.*

³²⁵ *Id.*

guidelines to guide parties through e-discovery disputes. Two good examples are (1) the U.S. District Court of Maryland's Suggested Protocol for the Discovery of Electronically Stored Information, which can be found at

<http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf>; and (2) the New York State Bar Association's "Best Practices In E-Discovery In New York State and Federal Courts," which can be found at

<http://www.nysba.org/AM/Template.cfm?Section=Home&ContentID=58331&Template=/CM/ContentDisplay.cfm>.

2. *Ensure That Social Media Is Preserved.* Facebook pages (for individuals and companies), web pages, tweets and electronic boards are often overlooked in current litigation hold notices. Make sure that the appropriate individuals at a client company have received litigation hold notices that specifically mention that, to the extent they may contain potentially relevant information, social media must be preserved. To the extent possible, have your e-discovery vendor, IT support personnel or client download a complete copy of any such social media as soon as a hold goes in place; impress upon them the fact that information cannot be deleted; and regularly check to make sure that no new data has been added and/or changed on the site during the course of litigation. Also, most social media sites operate by using cloud computing, which often has shorter electronic retention policies than most companies with dedicated server space. Be aware that since social media may involve outside organizations that operate with their own set of restrictions, it is important to start early.
3. *If Inadvertent Spoliation Occurs, Report It.* It is doubtful that the sanctions against Murray and Lester would have been as severe as they were if it were not for their repeated and systematic cover-up of the deleted information. Courts realize that the discovery of electronically stored information, while increasingly prevalent, still creates unique challenges. If counsel is able to make the case early on that the spoliation was inadvertent and that the party took reasonable steps to identify, recover and/or quantify the information lost, sanctions are likely to be less severe.
4. *Engage Competent Vendors and Counsel Early for Advice.* Make sure that your vendor has experience with collection and/or analysis of social media specifically, including preservation of associated metadata, and that your counsel likewise is on top of current social media issues that may affect your case. Importantly, while an e-discovery vendor should always be a key member of the discovery team, your outside counsel must be able to identify both technical and legal issues to make sure that the vendor is operating efficiently and effectively.³²⁶

CONCLUSION

The discovery rules for social media seem to be consistent in their application to a technology that is pervasive in our society. The Rules of Evidence remain intact – that if social media is to be used in a case, it must be relevant to the issue at trial and probative. What is somewhat new is that the nature of social media is that it provides a layer of privacy for the user – a layer that is controlled by the user. So, the courts have determined that in order to determine whether the material is relevant to the case, there must be some predicate or link to the case at hand. How that link is established may vary according to the nature of the case and how the

³²⁶ Landon, page 18.

social media was posted (whether in a private or public area of the social media site). However, the predicate can be established through the disclosures of the existence of the media by testimony, deposition, or an in-camera review of the evidence.

It is very likely that the court will serve as an intermediary whenever there is a dispute over the relevancy of the social media. It seems that the courts are going to require the parties to produce a predicate if one was not available through in-camera review of the potentially discoverable social media. It is just not conceivable that the courts will ever allow for the broad discovery of social media. No court is going to allow a fishing expedition, as was stated in the EEOC case, but at the same time, the courts recognize the potentially valuable material that is contained in social media sites.

Individuals once again need to be reminded that what they post in Facebook or other social media sites can be fodder for the opposing side in litigation. Attorneys need to exert care to not intentionally or unintentionally assist or order the spoliation of the social media.