Florida A & M University Law Review

Volume 9
Number 1 *Celebrating Our Legacy*

Article 10

Fall 2013

Social Media and Electronic Discovery: New Technology, Same Issues

Jesse C. Rowe

*Jesse C. Rowe**

SOCIAL MEDIA AND ELECTRONIC DISCOVERY: NEW TECHNOLOGY, SAME ISSUES

I. INTRODUCTION

In a generation of smartphones, wireless Internet, live streaming music and video chats, the modes of human communication are constantly evolving. One of the most popular forms of communication in recent years is the use of social media and social networking websites. Social media is a unique form of communication that involves not only the receipt of information, such as reading a newspaper or listening to the radio, but the transference of information between users. This back-and-forth exchange of information allows literally millions of people around the world to connect and interact with one another. Some social networking sites are designed for specific purposes, such as sending or receiving messages. Others, such as the popular Facebook and Twitter, incorporate a myriad of functions including the sharing of photographs and video, "status" updates, and GPS location "check-ins."

With all this information that is voluntarily published onto the Internet, there is no surprise that individuals seek to use this information during legal proceedings. For instance, an insurance company, defending itself against a lawsuit for personal injuries, may want to obtain pictures from the injured persons' social networking sites that show them behaving in a manner not consistent with their alleged injuries. A criminal defendant may want to prove his alibi by showing that his social networking sites' GPS locator places him far from the scene of the crime. These and countless other scenarios raise significant legal issues including what information can be "discovered," where this information can be obtained, and how it can be used.

The main purpose of this paper is to analyze how the discovery of social media and social networking sites during litigation presents the court system with very similar issues as traditional paper discovery. This new technology, however, forces the courts to address these

* J.D., 2014, Florida A&M University College of Law. The author would like to recognize the hard work and dedication of the College of Law's evening students who strive to balance employment, family, and legal education.

same issues in a different context. This discussion will first identify what discoverable information is and how the increase of electronically stored information has led to a new area of civil litigation discovery referred to as electronic discovery, or e-discovery. It will also examine the wide use and popularity of social networking sites and the explosion of discoverable information contained on them. As discussed below, the discovery of social media presents lawyers, judges and litigants with all too familiar issues including ethical concerns, scope and relevance of production, and privacy rights.

II. Federal Rules of Civil Procedure

A. Discoverable Information

The American system of justice allows for broad discovery of information that may be relevant to a particular legal issue. Discovery is defined as, "the pre-trial devices that can be used by one party to obtain facts in order to assist the party's preparation for trial."[1] These include, but are not limited to, requests for production of documents, deposition testimony and interrogatories. In a federal lawsuit, parties are required to automatically disclose certain information to each other without being asked, such as the names, addresses and telephone numbers of individuals likely to have discoverable information.[2] Such information must be relevant within the scope of discovery defined in the Federal Rules of Civil Procedure.[3] The rules state that, "parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[4]

Whether the discoverable information is admissible as evidence in court is a completely separate inquiry and subject to separate federal or state rules. "Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."[5] Therefore, discoverable information is not limited to evidence that is admissible at trial, but rather a broad amount of information that is relevant to the pending case.

1. Black's Law Dictionary 466 (6th ed. 1990).
2. Fed. R. Civ. P. 26(a)(1).
3. Fed. R. Civ. P. 26(b)(1).
4. *Id.*
5. *Id.*

B. *Emergence of Electronic Discovery*

Traditionally, discoverable information existed in the form of paper documents and tangible items. Lawyers on both sides of a dispute would gather and collect hundreds or even thousands of paper documents that would have to be organized and sorted for relevance. This would require a considerable amount of time and money, especially in complex litigation. However, as technology advanced, vast amounts of information began to be stored electronically. Organizations started compiling information in electronic databases and external hard drives, which allowed for a seemingly more practical way to sort and access large amounts of information. At first glance, electronic storage seemed to lend itself to efficiency, however, organizations soon found themselves requiring specialized computer programs, trained individuals, and even litigation departments devoted to managing the sheer volume of information stored.[6] "You've got new technology emerging that allows us to create and generate too much information and, as a consequence we've had to have new technologies emerge to manage that information."[7] Lawyers were left with little guidance as to what procedures applied to the discovery of electronically stored information.

This prompted the 2006 amendments to the Federal Rules of Civil Procedure that included the addition of "electronically stored information," or ESI. For example, Rule 34 now provides that a party may specifically request electronically stored information and specify the form in which the ESI is to be produced.[8] If a party does not specify the form, ESI may be produced in the form it is ordinarily maintained and the party need not produce ESI in more than one form.[9] Rule 45 also addresses ESI in regards to third party subpoenas. The rule states that a subpoena can specifically request the production of electronically stored information. However, "the person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost."[10]

---

6. SHIRA A. SCHEINDLIN, DANIEL J. CAPRA & THE SEDONA CONFERENCE, ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE (2d ed. 2012).

7. Jacquelyn Holt, *Social Media A Nightmare For E-Discovery*, ZDNET (Jan. 11, 2013, 2:40pm), http://www.zdnet.com/social-media-a-nightmare-for-e-discovery-1339304273.

8. FED. R. CIV. P. 34.

9. *Id.*

10. FED. R. CIV. P. 45.

Courts have applied the Federal Rules of Civil Procedural to electronically stored information in a similar manner as they would other types of discoverable information. As with paper documents and tangible items, parties have a duty to preserve electronically stored information when in reasonable anticipation of litigation.[11] The failure to preserve or destruction of electronically stored information can lead to sanctions for spoliation of evidence.[12]

III. Social Media

A. Popularity and Uses

More and more people are beginning to use social networking sites as one of their primary forms of communication. It is estimated that 91 percent of all adult internet users access or maintain social networking sites on a regular basis.[13] Recent statistical data from eBizMBA, an "eBusiness Knowledgebase" dedicated to tracking and ranking popular websites, cites the top 5 most popular social networking sites as 1) Facebook, with 750,000,000 estimated unique monthly visitors, 2) Twitter, with 250,000,000 estimated monthly visitors, 3) LinkedIn, with 110,000,000 estimated monthly visitors, 4) Pinterest, with 85,500,000 estimated unique monthly visitors, and 5) MySpace, with 70,500,000 estimated unique monthly visitors.[14]

Not only are people using social networking sites to communicate, they are also publishing vast amounts of their personal information to the public. It is estimated that every minute, Facebook users share 684,478 pieces of content; Tumblr blog owners publish 27,778 new posts; YouTube users upload 48 hours of new video; Foursquare users perform 2,083 check-ins; Flickr users add 3,125 new photos; and Instagram users share 3,600 new photos.[15]

---

11. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

12. *Id.*

13. Justine Murphy & Adrian Fontecilla, *Social Media Evidence In Criminal Proceedings: An Uncertain Frontier*, Bloomberg Law (Mar. 20, 2013), http://about.bloomberglaw.com/practitioner-contributions/social-media-evidence-in-criminal-proceedings-an-uncertain-frontier-by-justin-p-murphy-and-adrian-fontecilla.

14. *Top 15 Most Popular Social Networking Sites*, eBizMBA, http://www.ebizmba.com/articles/social-networking-websites (last visited Mar. 5, 2013).

15. Justine Murphy & Adrian Fontecilla, *Social Media Evidence In Criminal Proceedings: An Uncertain Frontier*, Bloomberg Law (Mar. 20, 2013), http://about.bloomberglaw.com/practitioner-contributions/social-media-evidence-in-criminal-proceedings-an-uncertain-frontier-by-justin-p-murphy-and-adrian-fontecilla.

Most of these social networking sites include basic components such as the ability to create a profile page, upload digital photographs and video, send public or private messages, and allow other users access to this information. Some sites allow for more detailed information to be published such as a user's education, current residence, and relationship status. These sites will also typically include their own search engine for finding people to connect with and social groups to join.

B. Social Networking Policies

Virtually every social networking site has some type of privacy policy in place to protect the information of its users from being disseminated to the public. Facebook gives users three options when sharing information. They can choose whether the information they post is available to the public, friends only, or a customized version of the two.[16] There are, however, many instances in which these privacy policies allow for user information to be shared for certain purposes, such as advertising or legal request, by virtue of simply enrolling for an account. For instance, the social networking site Instagram, which is primarily dedicated to the sharing of photographs, has a privacy policy that states, "[w]e may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so."[17] Instagram also states that ". . .you hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service. . ."[18] So, by signing up for a social media account with Instagram, a user expressly allows the site to share their personal photographs to third parties without notice or compensation.

Many sites have minimum age requirements, such as Facebook and MySpace, which require a user to be at least 13 years old to use the website.[19] LinkedIn, a social networking site dedicated to career professionals, requires that users be at least 18 years old to join and

16. *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/your-info (last visited Mar. 18, 2013).

17. *Privacy Policy*, INSTAGRAM, http://instagram.com/about/legal/privacy (last visited Jan. 29, 2013).

18. *Terms Of Use*, INSTAGRAM, http://instagram.com/about/legal/terms (last visited Jan. 29, 2013).

19. Susan Campbell, *Should Your Kids Use Social Media?*, REPUTATION, (Mar. 19, 2013, 9:32PM), http://www.reputation.com/reputationwatch/articles/should-your-kids-use-social-media.

used to require an invitation, but is now available for membership with a valid e-mail address.[20]

Most social networking sites also collect and store basic information about the user, such as the user's name, email address, birthday, and gender. Other information is frequently collected for supposedly enhancing the social networking experience. Facebook, for example, receives information when the user interacts with Facebook, such as whenever the user looks at another user's profile page, sends or receives a message, or posts photos and videos, including the metadata associated with each post (date, time and place).[21]

Some social networking sites have had their policies attacked on legal grounds for lack of notice. For example, Facebook is currently involved in a pending class action settlement that claims Facebook "unlawfully used the names, profile pictures, photographs, likenesses, and identities of Facebook users in the United States to advertise or sell products and services through Sponsored Stories without obtaining those users' consent."[22] The Electronic Privacy Information Center (EPIC) has also filed multiple complaints with the Federal Trade Commission (FTC) alleging that Facebook has engaged in unfair and deceptive trade practices by the way they share information with third-party application developers and by not making it clear to users that Facebook uses "cookies" to track their internet activity.[23]

IV. ETHICAL ISSUES

While much of the information posted on social networking websites is accessible to the public, some users exercise the option to allow their posts to be viewed by "friends only," or those that have been pre-approved by the user with permission to access their information. Thus, lawyers must be cautious in deciding how and when to obtain information contained on social networking sites.

The Philadelphia Bar Association's Professional Guidance Committee published an opinion in response to an inquiry regarding accessing a non-represented witness's social media accounts.[24] The at-

20. ENTREPRENEUR, http://social-media.entrepreneur.com/q/39/8525/What-are-the-requirements-to-join-the-LinkedIn-social-media-network (last visited Mar. 20, 2013).

21. *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/your-info (last visited Mar. 18, 2013).

22. Fraley v. Facebook, Inc., GCC, http://www.fraleyfacebooksettlement.com (last visited Feb. 6, 2013).

23. *Social Networking Privacy*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/socialnet/#back (last visited Mar. 14, 2013).

24. Philadelphia Bar Op. 2009-02 (Mar. 2009).

torney believed that the witness's Facebook and MySpace pages contained information that could be used to impeach her deposition testimony at trial.[25] The attorney sought to access this information directly but realized that he would need the witness's permission to do so.[26] Instead of asking the witness directly for permission to access her social networking sites (which she would most likely deny), the attorney proposed to have a third party "friend" the witness and report back to the attorney the information revealed.[27] The third party would not disclose the fact that he or she is only "friending" the witness simply to obtain personal information to supply the attorney with ammunition to impeach her testimony.[28] The attorney believed that this would be similar, in practice, to a private investigator following and videotaping a personal injury plaintiff.[29]

The Committee responded that, not only would this conduct violate two of the Committee's ethical rules, but also that it was highly deceptive. The Committed warned that,

> It omits a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness. The omission would purposefully conceal that fact from the witness for the purpose of inducing the witness to allow access, when she may not do so if she knew the third person was associated with the inquirer and the true purpose of the access was to obtain information for the purpose of impeaching her testimony.[30]

The New York State Bar published a similar opinion regarding the use of information posted on Facebook or MySpace pages by a party to a lawsuit, other than the lawyer's client.[31] In this scenario, the attorney did not propose to "friend" the party but to simply access what was already available to the public.[32] The Committee here relied primarily upon the previous opinion of The Philadelphia Bar Association's Professional Guidance Committee. However, they distinguished that the Philadelphia scenario concerned an unrepresented witness. Here, to the contrary, the target of discovery was an actual party.[33] The Com-

25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*
30. Philadelphia Bar Op., *supra* note 24.
31. New York Bar Op. 843, (Sept. 2010).
32. *Id.*
33. *Id.*

mittee went on to state that, "obtaining information about a party available in the Facebook or MySpace profile is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service. . .and that is plainly permitted."[34]

While the opinion did not specifically address this issue, the Committee made reference in a footnote that an attempt to "friend" a represented party could run afoul of the "no-contact" rule, which prohibits a lawyer from communicating with a represented party without the prior consent of that party's lawyer.[35] Ultimately, no ethical rules are violated by accessing a party's social networking site as long as the lawyer does not "friend" the party or direct a third person to do so.[36]

V. Battle In The Courtroom

A. Scope of Discovery

Parties frequently disagree on how much of their social networking site should be produced and whether their social networking sites should be produced at all. The court in *EEOC v. Simply Storage Management* recognized that there were not many published decisions to provide guidance on the issue of the discovery of social networking sites, but, nonetheless, applied the "basic discovery principles in a novel context."[37] In that case, the Equal Employment Opportunity Commission (EEOC) filed a complaint against Simply Storage Management (Simply Storage), alleging sexual harassment and damages for emotional pain and suffering, loss of enjoyment of life, post-traumatic stress disorder, and the like.[38] Simply Storage sent discovery requests seeking the production of essentially all of the claimants' social media content on Facebook and MySpace.[39] EEOC objected that the discovery requests were overbroad and not relevant.[40] The court began first by laying out general principles that could be applied to the discovery of social networking sites (SNS). They stated,

1. SNS content is not shielded from discovery simply because it is "locked" or "private.". . .

34. *Id.*
35. *Id.*
36. *Id.* at n.1.
37. EEOC v. Simply Storage Management, 270 F.R.D. 430 (S.D. Ind. 2010).
38. *Id.*
39. *Id.*
40. *Id.*

2. SNS content must be produced when it is relevant to a claim or defense. . .
3. Allegations of depression, stress disorders, and like injuries do not automatically render all SNS communications relevant, but the scope of relevant communications is broader than that urged by the EEOC.[41]

Reasoning that social networking sites may contain information that could reveal when and to what degree emotional injury occurred, the court held that the discovery of the claimants' social networking sites was appropriate.[42]

After establishing some workable guidelines regarding social networking sites, the courts' next challenge was to determine the scope of permissible discovery. Applying their established guidelines the court held that, ". . .the appropriate scope of relevance is any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and SNS applications. . .that reveal. . .any emotion, feeling, or mental state. . ."[43]

Similarly, in *Romano v. Steelcase*, the court granted the defendant's motion for access to the plaintiff's Facebook and MySpace accounts, including all previously deleted material.[44] In that case, the plaintiff brought a personal injury action in New York alleging damages for permanent injuries and loss of enjoyment of life.[45] The defendant found that the public portion of the plaintiff's Facebook and MySpace pages showed her smiling happily outside of her home and that she had traveled to Florida and Pennsylvania during the time period that she claimed her injuries were so severe she could not leave her home.[46] The court held that,

> In light of the fact that the public portions of plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action. Preventing defendant from accessing plaintiff's private postings on

41. *Id.*
42. *Id.*
43. Simply Storage, 270 F.R.D. at 436.
44. Romano v. Steelcase, 907 N.Y.S.2d 650 (2010).
45. *Id.*
46. *Id.*

> Facebook and MySpace would be in direct contravention to the liberal disclosure policy in New York State.[47]

While the above referenced cases indicate a trend towards broad discovery of social networking sites, the following case shows that the scope of discovery is not unlimited. In *Mackelprang v. Fidelity Nat'l Title Agency of Nev.*, the court denied the defendant's motion to compel a consent letter authorizing the defendants to access private messages contained on the plaintiff's two MySpace accounts.[48] In that case, the plaintiff sued her employer for, among other things, sexual harassment and intentional and negligent infliction of emotional distress.[49] The plaintiff alleged that two vice-presidents of the company coerced her into numerous sexual acts under the threat that she and her husband would be fired if she did not do so.[50] She also alleged that, as a direct result, she attempted to commit suicide twice, was hospitalized in a mental health facility, and was diagnosed with post-traumatic stress disorder, major depressive disorder, and panic disorder.[51]

During discovery, the defendants served a subpoena on MySpace for the production of private emails between the plaintiff and any other person.[52] MySpace responded with publicly available information but refused to produce the plaintiff's private emails without a search warrant or letter of consent.[53] Thereafter, defendants sent a "Consent and Authorization For Private Messages" letter to the plaintiff, which she refused to sign because the information they sought was "irrelevant and improperly invades plaintiff's privacy."[54] In their argument that the plaintiff was a willing participant and actually encouraged the alleged sexual misconduct, the defendant's pointed out that the plaintiff had two MySpace accounts, one that identified her as single with no kids and another that identified her as married with six children.[55] They also argued that,

> Mackelprang was using the private messaging functionality on MySpace to facilitate the same types of electronic and physical relationships she has characterized as sexual harassment in her Complaint. If in fact Mackelprang was voluntarily pursuing, en-

47. *Id.* at 654.

48. Mackelprang v. Fidelity Nat'l Title Agency of Nev., 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007).

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. Mackelprang, LEXIS 2379 at 6.

55. *Id.*

> couraging, or even engaging in extra-marital relationships on or though MySpace, then Fidelity has a right to use this information to rebut Mackelprang's sexual harassment claims and impeach her credibility.[56]

The district court disagreed and held that the defendants were engaging in a "fishing expedition" and would need something "beyond mere speculation" to support their claim.[57] The court reasoned that,

> Ordering plaintiff to execute the consent and authorization form for release of all of the private email messages on plaintiff's MySpace.com internet accounts would allow defendants to cast too wide a net for any information that might be relevant and discoverable. It would, of course, permit defendants to also obtain irrelevant information, including possibly sexually explicit or sexually promiscuous email communications between plaintiff and third persons, which are not relevant, admissible or discoverable.[58]

B. Relevance of Requested Discovery

Similar to the issue of the permissible scope of discovery, is the relevance of the requested information. As stated previously, relevant information need only be "reasonably calculated to lead to the discovery of admissible evidence."[59] Courts have shown the need to balance a party's right to obtain relevant information with a party's desire to protect such information from disclosure.

The court in *Barnes v. CUS Nashville, LLC* took a unique approach. There, the magistrate judge offered to create his own Facebook account and have two non-parties to which the discovery was directed accept him as a "friend" so that he could review their photographs and comments *in camera* to determine which, if any, contained relevant information.[60]

Similarly in *Bass v. Miss Porter's School*, the court reviewed over 750 pages of wall postings, messages, and pictures from the plaintiff's Facebook *in camera* to determine its relevance.[61] There, the plaintiff filed suit against her prep school for not protecting her against severe bullying and harassment.[62] The defendants sought production

56. *Id.* at 8.
57. *Id.*
58. *Id.* at 21.
59. FED. R. CIV. P. 26(b)(1).
60. Barnes v. CUS Nashville, LLC, 2010 U.S. Dist. LEXIS 143892 (M.D.Tenn.2010).
61. Bass v. Miss Porter's School, Civil No. 3:08CV1807, 2009 U.S. Dist. LEXIS 99916 (D. Conn. Oct 27, 2009).
62. *Id.*

of all communications related to the alleged teasing and taunting the plaintiff was subjected to on Facebook.[63] The plaintiff objected on the grounds that such information was irrelevant and immaterial, and not reasonably calculated to lead to the discovery of admissible evidence.[64] The court overruled the plaintiff's objection, holding that "Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting," therefore the Facebook communications were "clearly relevant."[65]

In contrast, the New York Supreme Court in *McCann v. Harleysville Ins. Co. of New York* held that the defendant's motion to compel authorization for the plaintiff's Facebook account and disclosure of photographs was properly denied as "overly broad."[66] In this uninsured/underinsured motorist action, the defendant alleged that the information contained on the plaintiff's Facebook account was relevant to determine if the plaintiff sustained serious injuries.[67] The court reasoned that since the defendant "failed to establish a factual predicate with respect to the relevancy of the evidence. . .defendant essentially sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence."[68] Nevertheless, the court did not preclude the defendants from accessing the plaintiff's Facebook account entirely. They held that, while the current motion to compel was properly denied, the lower court abused its discretion by prohibiting the defendant from seeking production of the plaintiff's Facebook account at some time in the future.[69]

C. Spoliation Sanctions

Another issue common to discovery is what to do when a party destroys or does not preserve discoverable information. As previously stated, the failure to preserve or the destruction of electronically stored information can lead to sanctions for spoliation of evidence.[70] These sanctions can include "dismissal of a claim or granting judgment in favor of a prejudiced party; suppression of evidence; an adverse infer-

63. *Id.*
64. *Id.*
65. *Id.* at 3-4.
66. McCann v. Harleysville Ins. Co. of New York, 78 A.D.3d 1524 (N.Y. 2010).
67. *Id.*
68. *Id.* at 1525.
69. *Id.*
70. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

ence, referred to as the spoliation inference; fines; and attorneys' fees and costs."[71] A spoliation inference "permits a jury to draw an adverse inference that the spoliated evidence might or would have been unfavorable to the position of the offending party."[72]

While there is little information available regarding spoliation sanctions in cases involving the failure to preserve information contained on social networking sites, the district court of New Jersey provides some guidance. In *Katiroll v. Kati Roll*, the court applied the usual requirements of a spoliation inference to the context of Facebook pages.[73] In this trademark infringement case, the plaintiff requested spoliation sanctions against the defendant for taking down his Facebook pages that contained infringing images and for changing his Facebook profile picture that displayed the infringing "trade dress."[74] The court applied a four factor balancing test: 1) the evidence must be within the party's control, 2) there must be actual suppression or withholding of evidence, 3) the evidence was relevant to claims or defenses, and 4) it was reasonably foreseeable that the evidence would be discoverable.[75] As to the second factor, some courts have held that the spoliation must be intentional to warrant an adverse inference instruction; while others have held that simple negligence is enough.[76] Here, the court held that the degree of fault should be based upon the amount of prejudice to the opposing party, that is, where the prejudice is substantial, negligence is sufficient to warrant a spoliation inference, and, where the prejudice is minimal, intentional conduct is required to warrant a spoliation inference.[77]

In weighing these factors, the district court concluded that there was not much at issue concerning the first and third factors, holding that the evidence was in the defendant's control and was relevant to the claim.[78] The main issues derived from factors two and four, the amount of fault and foreseeability, respectively. The court noted that "the change of a profile picture on Facebook is a common occurrence" and that "it would not have been immediately clear that changing [the defendant's] profile picture would undermine discovera-

71. Kounelis v. Sherrer, 529 F. Supp. 2d 503, 519 (D.N.J. 2008).
72. Veloso v. Western Bedding Supply Co., 281 F.Supp.2d 743, 746 (D.N.J. 2003).
73. Katiroll v. Kati Roll, 2011 U.S. Dist. LEXIS 85212 (D.N.J. Aug. 3, 2011).
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*

ble evidence."[79] The court ultimately held that, because of this, spoliation sanctions were inappropriate, but that the defendant should briefly change his profile picture back to the allegedly infringing picture so that the plaintiff's may print posts they believe to be relevant.[80]

While the *Katiroll* court did not impose sanctions for spoliation, its analysis is indicative of how courts will likely look at motions for sanctions regarding spoliation of information on social networking sites in the future.

D. Right to Privacy and the Stored Communications Act

"Probably the most frequently litigated issue surrounding discovery of social networking site information is the user's right to privacy."[81] It is undisputed that social networking sites contain personal information, but judges have struggled over when this personal information must be disclosed during litigation and when a person retains a right to privacy. Nonetheless, it seems that, for now, a person's right to privacy is diminished when it comes to information contained on social networking sites. For instance, a Canadian court recognized that,

> [t]o permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.[82]

Similarly, the *Romano* court recognized that,

> [A]s neither Facebook nor MySpace guarantee complete privacy, plaintiff has no legitimate reasonable expectation of privacy. . .[t]hus when plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.[83]

However, a person does not lose their right to privacy entirely simply because they share and communicate information on social networking sites.

---

79. Kati Roll, LEXIS 85212 at 10-11.
80. *Id.*
81. Kristen L. Mix, *Discovery of Social Media*, 5 Fed. Cts. L. Rev. 120, 127 (2011).
82. Leduc v. Roman, 2009 CanLII 6838 (ON S.C.).
83. Romano v. Steelcase, 907 N.Y.S.2d 650, 656-57 (2010).

1. Right of Privacy

The Fourth Amendment of the Constitution provides that, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . ."[84] The United States Supreme Court has interpreted this to mean that "the Fourth Amendment protects people, not places" where the person has a "reasonable expectation of privacy."[85] The Court applies a two-part test. First, a person must exhibit an "actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[86] They also reasoned that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[87]

In an attempt to apply this privacy right to electronically stored information, Congress enacted the Stored Communications Act (SCA) in 1986 as part of the Electronic Communications Privacy Act.[88]

> The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address. . . [It] creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information. . . Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection.[89]

2. Stored Communications Act Applied to Discovery of Social Media

The leading case on the Stored Communications Act and its applicability to social media is *Crispin v. Christian Audigier*.[90] In that case, an artist filed suit against a manufacturer of street-wear apparel alleging breach of contract and copyright infringement.[91] The defendants served subpoenas duces tecum on several social networking

84. U.S. CONST. amend. IV.

85. Katz v. United States, 389 U.S. 347 (1967).

86. *Id.* at 361.

87. *Id.* at 351.

88. 18 U.S.C. § 2701, et. seq.

89. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-13 (2004).

90. Crispin v. Christian Audigier, 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010).

91. *Id.*

websites, including Facebook and MySpace, seeking the production of, amongst other things, all communications that related to the plaintiff, defendant, or any of the sublicensee defendants.[92] The plaintiff filed a motion to quash the subpoenas on the grounds that the subpoenas were overbroad, sought irrelevant information, and sought electronic communications that were protected from disclosure under the Stored Communications Act.[93] The magistrate judge ruled that the Stored Communications Act did not apply because "the SCA prohibits only the voluntary disclosure of information by ECS [electronic communication service] providers, not disclosure compelled by subpoena."[94] The judge further concluded that third-party businesses are not ECS providers under the Act and the requested communications were not held in "electronic storage" as defined in the statute.[95]

On appeal, the district court recognized the difficulty in applying the Stored Communications Act to issues involving modern technology because "the SCA was enacted before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994."[96] They decided several issues regarding the SCA and discovery of social media including standing, whether the social networking sites are service providers under the statute, and whether the requested communications constitute electronic storage within the meaning of the statute.

a. Standing to Move to Quash a Third Party Subpoena Under the SCA

Rule 45 of the Federal Rules of Civil Procedure states that the court must quash a subpoena that "requires disclosure of privileged or other protected matter. . ."[97] "Ordinarily a party has no standing to seek to quash a subpoena issued to someone who is not a party to the action, unless the objecting party claims some personal right or privilege with regard to the documents sought."[98]

In the *Crispin* case, the defendants argued that the magistrate judge was correct in ruling that the plaintiffs did not have standing to move to quash the subpoenas duces tecum to Facebook and MySpace

92. *Id.*
93. *Id.*
94. *Id.* at 7.
95. *Id.*
96. *Id.* at 14.
97. FED. R. CIV. P. 45(c)(3)(A)(iii).
98. 9A CHARLES WRIGHT & ARTHUR MILLER, FEDERAL PRACTICE & PROCEDURE § 2459 (3d. ed. 2008).

because the Stored Communications Act states that, "[n]o cause of action shall lie in any court against any provider of wire or electronic communication service. . . in accordance with the terms of a court order, warrant, subpoena, statutory authorization or certification under this chapter."[99] The district court rejected the defendant's argument and held that the plaintiff did have standing to bring a motion to quash the subpoenas because "an individual has a personal right in information in his or her profile and inbox on a social networking site. . .the same way that an individual has a personal right in employment and bank records."[100]

b. Electronic Communication Service (ECS) Provider vs. Remote Computing Service (RCS) Provider

After determining that the plaintiffs had standing to move to quash the subpoenas, the district court then had to determine whether Facebook and MySpace are electronic communication service (ECS) providers or, alternatively, remote computing service (RCS) providers, under the Stored Communications Act. This determination was crucial to the case because ECS providers are prohibited from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[101] RCS providers are similarly prohibited from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service."[102] No court had previously decided whether social networking sites are ECS or RCS providers.

In making their determination, the court undertook a thorough analysis of the language of the statute. An ECS provider is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[103] An RCS provider is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[104] An electronic communications system is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or

99. 18 U.S.C. § 2703(e).

100. Crispin v. Christian Audigier, 2010 U.S. Dist. LEXIS 52832, 22 (C.D. Cal. May 26, 2010).

101. 18 U.S.C. § 2702(a)(1)(b).

102. *Id.* § 2702(a)(2).

103. *Id.* § 2510(15).

104. *Id.* § 2711(2).

electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[105]

The magistrate judge initially ruled that Facebook and MySpace were not ECS providers because their messaging services are used "solely for public display."[106] The district court disagreed and held that the sites are ECS providers because, first, the statute extends to "*any* service which provides to users thereof the ability to send or receive wire or electronic communications,"[107] and second, the sites provide private as well as public messaging.[108] They further reasoned that, "Facebook wall postings and the MySpace comments are not strictly 'public,' but are accessible only to those users plaintiff selects."[109] Therefore, "Facebook and MySpace provide an electronic venue to communicate. . ." and qualify as ECS providers prohibited from disclosing communications pursuant to the SCA.[110]

c. Electronic Storage

Since the district court found that both Facebook and MySpace are ECS providers under the SCA, their final inquiry was to determine if the requested communications constituted electronic storage under the statute.[111] The SCA defines electronic storage as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[112] The defendants argued that the requested communications did not constitute electronic storage because they are neither temporary in nature nor stored for backup purposes.[113] The district court disagreed and held that, "[a]s respects messages that have not yet been opened, those entities operate as ECS providers and the messages are in electronic storage. . .As respects messages that have been opened and retained by Crispin. . .[Facebook and MySpace] operate as RCS providers provid-

105. *Id.* § 2510(14).
106. Crispin v. Christian Audigier, 2010 U.S. Dist. LEXIS 52832, 41 (C.D. Cal. May 26, 2010).
107. 18 U.S.C. § 2510(15) (emphasis added).
108. *Id.*
109. *Id.* at 42.
110. *Id.* at 48.
111. *Id.*
112. 18 U.S.C. § 2510(17).
113. Crispin v. Christian Audigier, 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010).

ing storage services. . ."[114] Ultimately, the court granted the plaintiff's motion to quash the subpoenas seeking the Facebook and MySpace private messages but vacated and remanded to the magistrate judge the issue of whether the Facebook wall postings and MySpace comments are discoverable based on the plaintiff's privacy settings.[115]

The *Crispin* court demonstrated, for the first time, that the Stored Communications Act can be applied to the discovery of information contained on social networking sites and individuals can still retain some degree of privacy with respect to the information they choose to keep private.[116]

VI. CONCLUSION

The future of electronic discovery and social networking sites is moving forward at a rapid pace and the legal system is challenged to keep up. Fortunately, the Federal Rules of Civil Discovery have recognized the growth of e-discovery and have adopted amendments to address new concerns. Also, judges, lawyers and litigants are finding that traditional discovery issues are becoming more prevalent in the discovery of social networking sites. In the first half of 2012 alone, there were over 320 published cases where social media played a significant role.[117]

As demonstrated, the ethical and legal issues presented during discovery of electronically stored information in social media are nothing new to the court system. Lawyers must first ensure that they are not engaging in unethical behavior when seeking discovery of information contained on a party or witness's social networking site. State bar associations recognize that lawyers may easily obtain publicly available information but have little tolerance for misleading or deceptive tactics.

The electronic discovery requests themselves must be tailored to the appropriate scope and relevance of the claims or defenses at issue. Courts have recognized that, in many cases, social networking sites contain relevant information, but they will not let parties engage

114. *Id.* at 65.

115. *Id.*

116. *See also* Pietrylo v. Hillstone Rest. Group, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 5, 2009) (holding that restaurant managers maliciously accessing a private employee chat group on MySpace.com without authorization on five occasions warranted punitive damages under the SCA).

117. X1 DISCOVERY, *Published Cases Involving Social Media Evidence (First Half 2012)*, http://www.x1discovery.com/social_media_cases.html (last visited Mar. 5, 2013).

in "fishing expeditions" on a mere hunch that discoverable information could be located.

Courts have also shown their willingness to impose sanctions on parties who do not follow the rules of civil discovery. If discoverable information is not properly preserved or produced, the court may step in to punish the violating party and lessen the burden imposed on the prejudiced party. As judges become more familiar with social media and how social networking sites operate, sanctions may become more common with e-discovery violations.

The right of privacy will, undoubtedly, remain at the heart of many e-discovery issues. Parties will frequently argue that they retain a right of privacy to the information published on their social networking sites and opposing parties will frequently maintain that the need for such information outweighs the privacy interest. Although Congress has attempted to address these privacy issues in the Stored Communications Act, the 1986 federal statute is outdated and difficult to apply to modern day technologies. Judges ultimately have the responsibility of balancing the relevance of the information being sought against the privacy interest of the individual.

Even with this relatively new world of social media, these same legal issues still remain. It is the approach and application of the traditional rules of civil discovery to this new technology that makes electronic discovery of social networking sites such a unique and evolving area of the law.

Statement of Editorial Policy

The Florida A&M University Law Review is a journal that encourages thought-provoking scholarship by selecting articles that challenge existing assumptions and customary beliefs across a myriad of legal, cultural, and social issues. The opinions expressed in the included works are solely those of the contributing authors. The Florida A&M University Law Review and Florida A&M University do not necessarily share or endorse any particular views expressed in the articles published herein.