Facebook Me: E-Admissibility in the Internet Age

By: Dennis E. Sawan, Esq.
425 Jefferson Avenue Suite 910
Toledo, Ohio 43604
www.toledocounsel.com

567-343-5662

The following is provided free of charge to the public for general informational purposes only. Nothing in this work is intended as legal advice. If you have a specific legal issue or question, you are advised to seek out an Attorney.
Introduction

Whether or not the legal world is ready to admit it, social networking has and will continue to vastly change the landscape of the American judicial system. Facebook, the most popular social networking service in the world, reports that the website has over 600 million active users. 300 million of those users log on daily and in any given month, 700 billion minutes are spent on the social networking service. With these staggering numbers increasing daily, the evidentiary implications for the vast amount of electronic transmissions that occur at any moment are both groundbreaking and largely left undecided. As one Court notes, “despite the popularity of social networking services and the frequency with which this issue might be expected to arise, remarkably few published decisions provide guidance” EEOC v. Simply Storage Management, L.L.C., 270 F.Rd. 430, 432 (S.D. Ind. 2011). The following will explore this budding legal issue and how courts have dealt with the evidentiary concerns to date.

Social networking refers to “media for social interaction, using accessible and scalable communication techniques. Social media is the use of web-based mobile technologies to turn communication into interactive dialogues.” With the widespread adoption of the internet, more and more interpersonal communication is taking an interactive and, consequently, public form. With this come necessary questions regarding the evidentiary scope of such transmissions. The fate of these online communications in the legal process essentially distills down to two distinct questions, 1) are they discoverable? and, if so, 2) are they admissible?
Are Social Media Interactions Discoverable?

In the cases researched for the purposes of this paper, there does not seem to emerge a bright line rule regarding this question. However, it seems as if the majority opinion is that such transmissions are discoverable, however subject to the traditional limits of scope, privilege and proportionality. In making this determination, a trend of applying the classic approach to discoverability has begun to emerge. “Discovery of social networking site [transmissions] requires the application of basic discovery principles in a novel context.” *EEOC v. Simply Storage Management, L.L.C.*, 270 F.Rd. 430, 432 (S.D. Ind. 2011). To this end, the Court has been inclined to consider the following factors in addressing the question of discoverability:

1) Is it relevant to a party’s claim or defense?
2) Is the material sought subject to a privilege?
3) Does the material sought appear reasonably calculated to lead to the discovery of admissible evidence?
4) Is the discovery request proportional to the case?

*Fed. R. Civ. P. 26(b)(1); 26(b)(2)(C)*

To further understand each element of this analysis, it is important to view these questions through the lens of specific court proceedings. The first question above instructs a court to consider whether the social media interaction would be relevant to a party’s claim or defense. In other words, would the discovery of such online transmissions make it more or less probable that the allegation or defense is meritorious? To better understand how this works in the context of Facebook, it is helpful to consider the case of *EEOC v. Simply Storage Management, L.L.C.*, 270 F.Rd. 430 (S.D. Ind. 2011).
In this case, the Equal Employment Opportunity Commission brought suit on behalf of two named claimants and other similarly situated individuals for alleged sexual harassment that occurred at the workplaces of Simply Storage Solutions and O.B. Management Services L.L.C. Id. at 432. According to the claimants, the alleged harassment led to severe and ongoing emotional distress and depression. Id. While exchanging initial discovery, a significant dispute arose regarding the scope of the discovery of social networking communications. Id. At the base of this debate were the defendants’ requests for:

“All photographs or videos posted by Joanie Zupan or anyone on her behalf on Facebook or MySpace from April 23, 2007 to the present.

Electronic copies of Joanie Zupan's complete profile on Facebook and MySpace (including all updates, changes, or modifications to Zupan's profile) and all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, details, blurbs, comments, and applications for the period from April 23, 2007 to the present. To the extent electronic copies are not available, please provide the documents in hard copy form.

All photographs or videos posted by Tara Strahl or anyone on her behalf on Facebook or MySpace from October 11, 2007 to November 26, 2008.

Electronic copies of Tara Strahl's complete profile on Facebook and MySpace (including all updates, changes, or modifications to Strahl's profile) and all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, details, blurbs, comments, and applications for the period from October 11, 2007 to November 26, 2008. To the extent electronic copies are not available, please provide these documents in hard copy form.” Dkt. 38 Ex. 1.

The EEOC objected to the production of the aforementioned social networking content on the grounds that it was overbroad, unduly burdensome as it infringed on privacy interests, and would harass and embarrass the claimants. Id. The defendants countered by claiming that the discovery was necessary in order to properly dispute the
allegations that the claimants suffered “emotional pain and suffering, loss of enjoyment of life, anxiety, fear, bitterness, humiliation, embarrassment and inconvenience.” *Id.* at 433. Therefore, the court was given the task of defining, “appropriately broad limits--but limits nevertheless - on the discoverability of social communications in light of a subject as amorphous as emotional and mental health, and to do so in a way that provides meaningful direction to the parties.” *Id.*

The court began the analysis of this issue by citing Rule 26(B) of the Federal Rules of Evidence. *Id.* The Court notes that this is a broad standard of discovery, reiterating that "[W]here relevance is in doubt, [Rule 26(b)(1)] indicates that the court should be permissive." *EEOC v. Simply Storage Management, L.L.C.,* 270 F.Rd. 430, 433 (S.D. Ind. 2011) citing *Truswal Systems Corp. v. Hydro-Air Engineering, Inc.,* 813 F.2d 1207, 1212 (Fed. Cir. 1987). The EEOC in this matter was not arguing that the information sought by the defendant was irrelevant and therefore should be precluded altogether. *EEOC v. Simply Storage Management, L.L.C.,* 270 F.Rd. 430, 433 (S.D. Ind. 2011). Rather, they argued that a narrowing of the scope to those communications that directly referred to the matter alleged in the complaint was required. *Id.* In contrast, the defendant asserted that since the claimants emotional health over a wide range of time is put at issue by the nature of the claim, all transmissions via social networking are relevant to the exercise of a potentially meritorious defense. *Id.* The court in this matter was somewhat hesitant to extend the type of breadth of discovery that the Defendants were seeking. As the Court explains, “ anything that a person says or does might in some theoretical sense be reflective of her emotional state. But that is hardly justification for requiring the production of every thought she may have reduced to writing or, indeed, the
deposition of everyone she may have talked to.” *EEOC v. Simply Storage Management, L.L.C.*, 270 F.Rd. 430, 433 (S.D. Ind. 2011) citing *Rozell v Ross-Holst*, 2006 U.S. Dist. LEXIS 2277, 2006 WL 163143 (S.D.N.Y. Jan. 20, 2006). However, in recognizing this, the court did find that there was a need for some degree of discovery of social networking transmissions. “It is reasonable to expect severe emotional or mental injury to manifest itself in some social networking site content, and an examination of that content might reveal whether onset occurred, when, and the degree of distress. Further, information that evidences other stressors that could have produced the alleged emotional distress is also relevant.” *Id.* Therefore, the Court found that discovery of this type of information is permissible and required, but required a deeper analysis into the appropriate scope.

They begin this meditation into the appropriate scope by stating that the EEOC’s proposal is unworkable, as confining discovery to those matters that “directly reference the matters alleged in the complaint is too restrictive.” *Id.* The court elaborates by explaining that people are unlikely to communicate non-events through social networking. (For example, “today I was not harassed at work) *Id.* Confining the discovery to the scope EEOC proposes would ultimately preclude the discovery of a significant amount of highly relevant data regarding the claimants’ emotional and mental state. Ultimately, the court concluded that, “With these considerations in mind, the court determines 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 social networking site applications for claimants Zupan and Strahl for the period from April 23, 2007, through the present that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or
relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state.” *Id.* at 437. The court further explains that this rule can apply to nearly anything posted on social networking sites, including photographs. *Id.*

Lastly, the court considered the EEOC’s privacy concerns raised in its objection to the discovery request. The court noted “that this is the inevitable result of alleging these sorts of injuries [emotional distress]. Further, the court finds that this concern is outweighed by the fact that the production here would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through [social network] postings.” *Id.* This is perhaps the most enlightened realization the court in this case has come to. In doing this, the court reiterated what one Judge explained, that is that "Facebook is not used as a means by which account holders carry on monologues with themselves." *Leduc v. Roman*, 2009 CanLII 6838 (ON S.C.). This unique nature of social networking is critical to the general accessibility of the transmissions through discovery. In the future, this reality is likely to largely preclude the objection to discovery of social networking data as overly invasive of privacy.

Parties in lawsuits have not been the only ones to raise privilege arguments regarding social networking communications. Often times, social networking services themselves seek to be shielded from discovery requirements. These arguments are somewhat, albeit not much, more fruitful than when an individual seeks to assert a privilege based on privacy. The most common privilege asserted by social networking service providers is the Stored Communications Act 18 U.S.C § 2702(a). The SCA generally prohibits the disclosure of stored electronic communications by an electronic
communication provider without certain exceptions. 18 U.S.C 2702. “The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.” Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008). In the case of Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. May 26, 2010), the argument was raised that the SCA general prohibitions precluded the compliance with subpoenas by social networking services. Id. at 971. The court ultimately concluded that the SCA does limit disclosure as to private communications, and remanded the case with reference to the more public communications. Id. at 991. One of the important points to note from this case is that the dated approach to the issues underlying the Stored Communications Act makes it exceedingly difficult to apply it to the landscape of the modern day internet. Id. The Court notes that the statute creates different levels of disclosure standards based on an identification of a service as either a remote computing service (“RCS”) provider or an electronic communication service (“ECS”) provider. Id. at 972. The SCA defines an ECS provider as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). With certain exceptions, the SCA prohibits an ECS provider from “knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service.” Id., §§ 2702(a)(1), (b). This definition and prohibition seems to allude to a service which is temporal in nature. “The SCA defines RCS as “the provision to the public of computer storage or processing services by means of an electronic communications system,” id., § 2711(2), and in turn defines an electronic communications system (as opposed to an electronic communication service) as “any wire, radio, electromagnetic, photooptical or
photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications,” id., § 2510(14).” Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. May 26, 2010) [Emphasis added]. The SCA prohibits an RCS provider from “knowingly divulging] to any person or entity the contents of any communication which is carried or maintained on that service.” 18 U.S.C. § 2702(a)(2).

Based on this, it appears that when congress enacted the SCA, they intended on differentiating different standards depending on the longevity of the storage with the service provider. However, while this may have made sense in 1986 when the act was passed, it is somewhat unworkable to the current legal issues regarding social networking.

“The difficulty in interpreting the statute is “compounded by the fact that the [SCA] was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [Facebook and MySpace]. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.” As the Ninth Circuit further observed, “until Congress brings the laws in line with modern technology, protection of the Internet and websites such as [these] will remain a confusing and uncertain area of the law.” Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. May 26, 2010) citing Konop, 302 F.3d at 874.

The problem raised by the court here is that the SCA was passed in 1986 when the internet was very much in its infancy. A user would log on to the internet sporadically and would generally only remain online for a short period of time. To further explain, “the SCA was enacted before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994.” William Jeremy Robison, Note, Free at What
Cost? Cloud Computing Privacy Under the Stored Communications Act, 98 Geo. L.J. 1195, 1196 (2010) As a result, the SCA “is best understood by considering its operation and purpose in light of the technology that existed in 1986. The Act is not built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress chose to draft a complex statute based on the operation of early computer networks. To apply the Act to modern computing, courts need to begin by extracting operating principles from a tangled legal framework.” Id. This incredibly dated language in the statute is likely to render the protections of the SCA to social networking providers difficult at best, obsolete at worst. As a result, it seems overtly necessary for congress to address the problems in the application of the SCA if it wishes to ensure the preservation of the rights the act initially sought to protect. As one scholar noted, “Although the SCA was not intended to be ‘a catch-all statute designed to protect the privacy of stored Internet communications,’ it has been pressed into this role. Without the SCA to balance the interests of users, law enforcement, and private industry, communications will be subjected to a tug-of-war between the private companies that transmit them and the government agencies that seek to access them. Internet users will find themselves with little protection.” Nathaniel Gleicher, Neither a Customer nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web, 118 Yale L.J. 1945, 1945 (2009)

The last two concerns the court instructs are pertinent to this analysis are the degree the discovery request is reasonably calculated to lead the discoverability of admissible data and the proportionality of the request. The question of admissibility will be largely covered in the next section of this paper, and unfortunately since this issue is in
it’s infancy, is left with more questions than answers. The question of proportionality is very pertinent to this area of law, as Courts are often asked to weigh a social networking users privacy interests in contrast to a defendants’ necessity to gain information relevant to their defense. For example, the case of Romano v. Steelcase, Inc., 30 Misc. 3d 426, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010) is an illustration of the inquiry into proportionality. In this case, a plaintiff brought suit against Steelcase Incorporated for personal injuries sustained. Id. Among the damages alleged was the contention that the injuries sustained were of such a character as to substantially affect the plaintiff’s quality of life. Id. The Defendant requested access to the Plaintiff’s current and historical Facebook and Myspace pages and accounts, included all deleted pages, on the grounds that the content may provide evidence to refute the plaintiff’s claims concerning the extent and nature of her injuries and claims for loss of enjoyment of life. Id. The Defendant further contended that despite the Plaintiff’s claims, photographs posted on her Facebook and Myspace profile show her in vacationing in Florida and Pennsylvania and engaging in activities in contradiction to her claim of loss of enjoyment. Id. As the Court notes, “plaintiff’s public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed.” Id. The Court was not swayed by the Defendant’s argument that a balance of the interests at issue here required the protection of the Plaintiff’s privacy. The Court in this case cited to a popularly cited Canadian case reaffirming that, “To 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” *Leduc v. Roman, 2009 CanLII 6838 (ON S.C.).* Further, in determining a right to privacy, the Court reiterated a two part test; in order for a fourth amendment right to privacy to exist, “first… a person [must] have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable” *Katz v United States, 389 US 347, 351 [1967].* “Whether one has a reasonable expectation of privacy in Internet postings or e-mails that have reached their recipients has been addressed by the Second Circuit, which has held that individuals may not enjoy such an expectation of privacy (*see United States v Lifshitz, 369 F3d 173, 190 [2004]*) *Id. at 433.* Therefore, the Court found that the Plaintiff had no right to an expectation of privacy and thus was required to provide the Defendant with access to her profile.

In summation, it appears that certain generalities regarding the discoverability of social network transmissions have surfaced. For one, it seems as if the majority opinion is that such transmissions are discoverable, so long as they are relevant to a claim or defense and not privileged or disproportionate. Secondly, it seems safe to say that the Stored Communications Act will prevent involuntary disclosure by service providers generally, but its language is incredibly dated and at risk of becoming obsolete and unworkable. Lastly, it appears that an expectation of privacy in the context of internet postings is not a valid defense to their discoverability.
Are Social Network Transmissions Admissible?

As opposed to the rules that emerge regarding discoverability, admissibility is a much more challenging topic with respect to social media. A legal analysis into this topic seems to leave more questions than answers. In order to have social media information admitted into evidence, a proponent must establish that the information is relevant, authentic and does not violate either the hearsay or best evidence rule. In an ideal circumstance, the proponent of the admission of evidence can obtain a stipulation for much of the groundwork. However, where this is not possible, establishing authenticity can be exceedingly challenging. This is due to the fact that, as on Federal Judge commented, “anyone can put anything on the internet… [the internet is] one large catalyst for rumor, innuendo, and misinformation” St. Clair v. Johnny’s Oyster & Shimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999). It is “voodoo information”. Id. at 775.

Two major hurdles for the admissibility of social networking site content are timeliness and authorship. Joshua A. Norris & Krystal Pfluger Scott, How to Authenticate Social Networking Sites, The Legal Intelligencer, Feb 4, 2011. The difficulty with timeliness is that it can be difficult to prove that content added was done so in the relevant timeframe. Perhaps even more difficult is proving that a photograph posted on a social networking site was taken within close proximity to its publication. Absent a stipulation, these hurdles can become unsurpassable. Authorship is also difficult to establish when disputed due to the general accessibility of the internet.
Generally, the Federal Rules of Evidence are applicable to such questions of authentication. Federal Rule of Evidence 901(a) establishes that “the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.” The rule goes on to provide illustrations of examples of proper authentication including “testimony of a witness with knowledge that a matter is what it is claimed to be” and “distinctive characteristics and the like, appearance, contents, substance, internal patterns or other distinctive characteristics, taken in conjunction with circumstances.” Fed. Rule 901(b)1, 4. In application, this rule means that it may be possible to authenticate timeliness or authorship of social networking transmissions by various methods. For one, a proponent for admissibility may be able to find a witness who was present at the time the transmission was made or photograph was taken. Secondly, it may be possible that the particular transmission at issue bears such a distinct character as to be reasonably attributed to other stipulated transmissions, and as such authenticated. The case law is incredibly scant regarding this issue, but the case of *Lorraine v. Markel Insurance American Company* distills the federal rule in the context of online transmissions. This case lays out a set of questions that must be answered before website evidence is admissible. These questions are:

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 website or profile page?

These questions were litigated in the case of Tienda v. State, No. 05-09-00553-CR, 2010 Tex. App. LEXIS 10031 (Ct. App. Dec. 17, 2010). In this criminal case, the Defendant was charged and convicted of murder. *Id.* Myspace content was admitted into evidence, over the Defendant’s objections that there was no proof that the pages at issue were created and maintained by him. *Id.* The Appellate Court was influenced by the language in Federal Rule of Evidence 901(b)4 which allowed an inquiry into the circumstances surrounding a transmission for the purposes of authentication. *Id.* In this case, the Myspace content in this matter showed that the owner referred to himself as “Smiley” or “Ron Tienda, Jr. in Dallas” or “D-Town”. *Id.* There were photographs of appellant on the pages in question and references to the murder, placement on electronic monitoring and comments regarding arrest. *Id.* The court said,

> “the inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds and lifestyles. This type of individualization is significant in authenticating a particular profile page as having been created by the person depicted in it. The more particular and individualized the information, the greater the support for a reasonable juror’s finding that the person depicted supplied the information.” *Id.* at 12-13.

This case begins to lay the foundation for an evidentiary carve-out specific to social networking. As time passes, the legal issues surrounding the transmissions of online communications will necessarily become further meted out. As the nature of these communications is better understood in our legal system, and legislators continue to adapt to new technologies, the unanswered questions will likely become much clearer. For now, however, questions of admissibility require a novel approach and a degree of creativity in laying the appropriate foundation.