ALFA International
The Global Legal Network
Celebrating 40 Years

THE INS AND OUTS OF SOCIAL MEDIA IN LITIGATION

AUTHORED BY ALFA INTERNATIONAL ATTORNEYS:

Janelle Kilies
LEWIS WAGNER
Indianapolis, IN
jkilies@lewiswagner.com

William (Skip) Martin
HAIGHT BROWN & BONESTEEL LLP
Los Angeles, CA
wmartin@hbblaw.com

ALFA International
The Global Legal Network
Celebrating 40 Years

THE INS AND OUTS OF SOCIAL MEDIA IN LITIGATION

INTRODUCTION

Generally speaking, social media can be used both offensively and defensively in litigation. Offensively, we will discuss how to ethically obtain social media from your opponent and what to do with it once you have it. Defensively, we will cover ways to defend against the use of your own company's (or employees) social media sites in litigation.

SOCIAL MEDIA AND THE STANDARD OF THE COURTS

Prior to ordering discovery, many courts require a showing of relevance before they order social media discovery. *Alexandra D. Jones, Forman v. Henkin: The Conflict Between Social Media Discovery and User Privacy*, 7 Cal. L. Rev. 30, 32 (2016). Therefore, the party seeking discovery must find relevant information in the public portion of the opposing party's social media to establish relevance to access the private portion. Id. "Other courts take a broader view of relevancy, as one court found that 'photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy setting that the user may have established.'" *Id*.

Once the seeking party has established relevance, most courts limit access through an in-camera review prior to production or by expressly limiting production to clearly relevant information, absent an in-camera review. *Id*. Some courts have decided to permit unfettered access by ordering the producing party to provide his or her social media login information. *Id*.

A recent opinion from the New York Court of Appeals offers guidance related to the discoverability of social media. In *Forman v. Henkin*, 30 N.Y.3d 656, 666 (2018) the court offered the following criteria to evaluate whether social media was discoverable: (1) consider the nature of the event causing the litigation and the injuries claimed to assess whether relevant material is likely to be found on the social media account, and (2) issue an order tailored to the particular controversy, balancing the potential utility of the information sought against any specific "privacy" or other concerns raised by the account holder. *Id*. at 665. This standard resembles the proportionality considerations now used by federal courts and explicitly encouraged by the New York Commercial Division. Harold K. Gordon et. al., *New York's Top Court Rules 7-0: "Private" Facebook Posts Subject to Disclosure*, JONESDAY (Feb. 2018), https://www.jonesday.com/new-yorks-top-court- rules-70-private-facebook-posts-subject-to-disclosure-02-22-2018/.

OFFENSIVE DISCOVERY

How to Obtain Social Media Discovery Ethically

Preservation of Evidence Letter

Any time a potential claim arises, an attorney should consider sending an evidence preservation letter to opposing counsel to maintain possible social media evidence (among other potentially relevant evidence). Laurel E. Stevenson, *Social Media: Practice Tips and Case Law Developments*, 73 J. Mo. B. 78, 79–80 (2017). A preservation letter advises of the possibility of future litigation and identifies relevant documents and electronically stored information which should be preserved. Stephanie F. Stacy, *Litigation Holds: Ten Tips in Ten Minutes*, UNITED STATES DISTRICT COURT OF NEBRASKA 1, https://www.ned.uscourts.gov/internetDocs/cle/2010-07/LitigationHoldTopTen.pdf.

When drafting a preservation letter, "it should be appropriately tailored, much like discovery is required to be tailored." Laurel E. Stevenson, *Social Media: Practice Tips and Case Law Developments*, 73 J. Mo. B. 78, 79–80 (2017). Failure to comply with a preservation letter will subject the non-compliant party and/or attorney to spoliation claims and sanctions from the court. *See generally Stephanie F. Stacy, Litigation Holds: Ten Tips in Ten Minutes*, UNITED STATES DISTRICT COURT OF NEBRASKA 1, https://www.ned.uscourts.gov/internetDocs/cle/2010-07/LitigationHoldTopTen.pdf.

Formal Discovery

When seeking formal social media discovery from an opposing party, attorneys should consider the parameters of any request, not unlike the parameters applicable to the discovery of health care information in a personal injury lawsuit (e.g., limited to a time period and to certain sources). Laurel E. Stevenson, *Social Media: Practice Tips and Case Law Developments*, 73 J. Mo. B. 78, 80 (2017). For example, Missouri courts have held that parties are not allowed to engage in unlimited discovery or fishing expeditions under Rule 56.01 of the Missouri Rules of Civil Procedure. *Id*. Where courts permit only approved written discovery, attorneys should agree with opposing counsel to go beyond the court's approved discovery if it does not include social media evidence. *Id*. If an agreement cannot be reached, an attorney "should consider filing a motion for leave to obtain social media discovery." *Id*.

A New Jersey case highlights the need for exercising caution when accessing social media accounts during pending litigation. Laurel E. Stevenson, *Social Media: Practice Tips and Case Law Developments*, 73 J. Mo. B. 78, 81 (2017). In *Gatto v. United Air Lines, Inc.*, the plaintiff deactivated his Facebook account, and "Facebook . . . 'automatically deleted' the account fourteen days after its deactivation." No. 10-CV-1090- ES-SCM, 2013 WL 1285285, at *2 (D.N.J. Mar. 25, 2013). The *Gatto* court concluded that the plaintiff "failed to preserve relevant evidence" and instituted a spoliation sanction against the plaintiff, resulting in an adverse inference instruction. *Id*. at *5. "To avoid [] unintended consequences, parties may [] consider using an independent provider to access the information or have the information provided to the court for [in-camera] review before disclosure to the other side." Laurel E. Stevenson, *Social Media: Practice Tips and Case Law Developments*, 73 J. Mo. B. 78, 81 (2017).

Requests for Production of Documents

When sending requests for production of documents, attorneys should remember two important limiting factors: "(1) a request for production must describe the documents sought with 'reasonable particularity' and, (2) in order to request social media information 'behind the privacy wall,' you must locate evidence on the public-facing pages that lead you to the existence of relevant evidence behind that wall." Emily Miskel and Britney Harrison, *IV. HOW TO REQUEST AND GET SOCIAL MEDIA IN DISCOVERY*, 2018 TXCLE-AFL 57-V, 2018 WL 6366759 (2018). Thus, requesting parties need to be particular about the social media needed for litigation. *Id*.

A case from Texas sheds light on this issue. In I*n re Indeco Sales, Inc.*, a Texas state court considered the following requests for production in dispute:

> (1) A color copy of any and all photographs and/or videos of you (whether alone or accompanied by others) posted on your Facebook page(s)/account(s) since the date of the accident on August 23, 2013.

> (2) A color copy of all Facebook posts, Facebook messages and/or Facebook chat conversations, other than those protected by the attorney-client privilege, authored, sent or received, and/or otherwise entered into by you since August 23, 2013.
>
> (3) A color copy of any and all photographs and/or videos of you (whether alone or accompanied by others) posted on your Facebook page(s)/ account(s) prior to August 23, 2013.
>
> (4) A color copy of all Facebook posts, Facebook messages and/or Facebook chat conversations, other than those protected by the attorney-client privilege, authored, sent or received, and/or otherwise entered into by you prior to August 23, 2013.

In re Indeco Sales, Inc., 09-14-00405-CV, 2014 WL 5490943 at *1-*2 (Tex. App. – Beaumont Oct. 30, 2014, no pet.). "The Court of Appeals [held that] the trial court did not err in sustaining the objections to these requests as overbroad or in denying realtors motion to compel." *Id*. at *2. The court noted that the first request for production requested that the plaintiff produce every photograph and video posted since the date of the accident regardless of when the photograph was taken or created. *Id*. The second request for production required the plaintiff produce every post, message, or chat conversation authored, sent, or received by her, no matter how mundane or remote, regardless of the topic, content, or subject. *Id*. Although some limits were placed on the time period, no limit was placed on the scope of the request or the subject matter of the post, which made the request overbroad. Id. Side note: when defining the time period for social media information, you must be sure to specify the time period by the date the photos were taken rather than the date they were posted. *Id*.

Bottom line: "If you are looking for something specific, spell it out." *Id*. "For example, if you want a party to download and produce his Twitter archive, set forth the instructions in the discovery request." *Id*. It is all too common for a blanket request to not include electronically stored information (ESI) requests. *Id*. "'It is the discovery proponent's burden to demonstrate that the requested documents fall within the scope-of-discovery.'" Id. The burden should not be on the court to redraft the overly broad requests. *Id*.

What if the Party Refuses?

Your best bet is to file a motion to compel seeking an order requiring a party to execute an authorization for the requested information. Given the sensitive nature of private ESI, the requesting attorney should consider agreeing to a protective order to shield the opposing party from embarrassment and to maintain the private nature of the ESI.

An attorney may attempt to subpoena social media information when the opposing side refuses to hand over the relevant information. However, the Stored Communications Act (SCA), 18 USC § 2701 et. seq., restricts obtaining electronic communications by subpoena. "The SCA does not allow disclosure of electronic communications in response to a civil subpoena in the same manner as it does for ongoing criminal investigations." Miskel, *supra*. Facebook's policy on civil subpoenas reads: "Federal law does not allow private parties to obtain the content of communications (example: messages, timeline posts, photos) using subpoenas." *See* the Stored Communications Act, 18 U.S.C. § 2701 et seq." *Law Enforcement & Third-Party Matters*, Facebook, https://www.facebook.com/help/473784375984502.

What Not to Do

An attorney or the client should not friend or advise another person on his or her behalf to friend an opponent. Model Rule 8.4 of Professional Conduct states that a lawyer cannot:

> (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;
>
> (b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;
>
> (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation . . . .

Model Rules of Prof'l. Conduct R. 8.4. Accordingly, the Philadelphia Bar Association Professional Guidance Committee issued an ethics opinion that declared attorneys friending or directing their staff to friend deponents on Facebook is unethical. Heather L. King et. al., *When Evidentiary Matters Cross Ethical Boundaries*, 57 S. Tex. L. Rev. 527, 536 (2016). The Guidance Committee stated that such "friending" is misconduct because it is dishonest, misleading, and fraudulent conduct because "the person attempting to friend the deponent would omit highly material facts in their communication, such as the fact that the person is associated with the attorney, such request would be a violation of the Pennsylvania Rules of Professional Conduct." *Id*. at 535-36. Such dishonest conduct would likely violate the Model Rules of Professional Responsibility.

Scanning the public portion of a party's social networking site is not an ethical violation. *Id*. at 536. However, the New York State Bar Association's Committee on Professional Ethics outlined a twofold ethical approach over the private portion of a party's social networking site: first, it stated that by attempting to "friend" a represented party, the attorney would violate the no-contact rule of ethics, and second, if the attorney attempted to "friend" an unrepresented party, the attorney would be required to clarify the lawyer's role and refrain from giving any legal advice. *Id*.

Do Attorneys Have a Duty to Disclose Information? And if so, when?

The duty to preserve relevant evidence—either paper or electronic—may trigger when (1) civil litigation is commenced, or (2) civil litigation is reasonably anticipated. *Zubulake v. UBS Warburg*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

First, when litigation commences, the duty to preserve exists for a defendant, at the latest, when the defendant is served with the complaint. *NuCor Corp. v. Bell*, 251 F.R.D. 191, 197 (D.S.C. 2009). In most cases, the duty to preserve evidence is triggered by the filing of a lawsuit. *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc*., 244 F.R.D. 614, 621 (D. Colo. 2007). A formal discovery request is not necessary to trigger the duty to preserve. *Krumwiede v. Brighton Assocs., LLC*, No. 05-C-2003, 2006 WL 1308629 (N.D. Ill. May 8, 2006).

When litigation is reasonably anticipated, the duty to preserve evidence attaches when a party reasonably knows that the evidence may be relevant to litigation. *Silvestri v. General Motors*, 271 F. 3d 583, 589 (4th Cir. 2001). However, for plaintiffs, their duty is more often triggered before litigation commences because plaintiffs control the timing of litigation. *Pension Comm. Of the Univ. of Montreal Pension Plan v. Banc. Of Am. Sec. LLC* ("Pension Committee"), 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

Because plaintiffs control the timing of litigation, they also have pre-litigation obligations regarding the preservation of evidence. For instance, the Florida Bar published an opinion, offering guidance on the matter:

> A lawyer may advise a client to use the highest level of privacy settings on the client's social media page. A lawyer may also advise the client pre-litigation to remove relevant information from the client's social media page so long as the removal does not violate any substantive law regarding preservation and/or spoliation and the information is preserved.

Florida Bar Ethics Opinion 14-1 (June 25, 2015). New York also published a similar advisement:

> But provided that such removal does not violate substantive law regarding destruction or spoliation of evidence, there is no ethical bar to "taking down" such material from social media publications, or prohibiting the client's attorney from advising the client to do so, particularly inasmuch as the substance of the posting is generally preserved in cyberspace or on the user's computer.

NYCLA Ethics Opinion 745, Advising a Client Regarding Posts on social Media Sites (July 2, 2013).

Once a duty is triggered to preserve discoverable social media, parties must then consider the scope of discovery. To determine the scope, relevance is a key consideration. Discovery relating to social media "requires the application of basic discovery principles in a novel context." *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430 (S.D. Ind. 2010). "Where there is an indication that a person's social network sites contain information relevant to the prosecution or defense of a lawsuit . . . access to those sites should be freely granted." *McMillan v. Hummingbird Speedway*, No. 113-2010 CD, 2010 WL 4403285 (Pa. C.P. Jefferson Sept. 9, 2010). With these basic ideas in mind, the view of relevance has evolved.

Generally, relevance in one case does not necessarily equate to relevance in another case. In a personal injury case, "the fact that plaintiff had previously used Facebook to post pictures of herself or to send messages is insufficient to warrant discovery of this information." *Kelly Forman v. Mark Henkin*, 2015 N.Y. App. LEXIS 8353 (Dec. 17, 2015). Simply because the plaintiff's Facebook postings "might reveal daily activities that contradict claims of disability" is "nothing more than a request to conduct a fishing expedition." Id. Another case took a broader view of relevance where in a slip and fall case, the plaintiff took down hundreds of photographs from his Facebook page following the deposition. *Nucci v. Target Corp.*, 162 So.3d 136, 154 (Fla. 4th DCA 2015). The appellate court upheld the trial court order requiring production of photographs from two years prior to the incident. *Id*. "We agree with those cases concluding that generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings that the user may have established." *Id*. Yet, another court disagreed that the entirety of a plaintiff's social media account is per se relevant to any claim of emotional distress damages. *Amalya Thurmond v. Margaret Bowman, et al.*, 2016 U.S. Dist. Lexis 45296 (W.D.N.Y. Mar. 31, 2016). Social media postings may be relevant to claims or defenses "where social media posts may contradict claims of physical or emotional injury." *Id*.

Major social media websites such as Facebook, Twitter, and Instagram, have made preserving data from social media accounts simple. For example, please see the following instructions regarding how to preserve data on Facebook:

> It is important that the client understands the power of settings in Facebook, and that the client actually uses them. Instruct the account holder (client) to go into "Settings" of their Facebook account and navigate to the ""Backup" screens/menus. Here the account holder can preserve, at that point in time, the complete history and the entire content of a Facebook account holder's account with all posts, time lines, and everything in the account. So it is preserved before it is "hacked" or bogus postings appear. Go to Home, Settings, then Click "Download a copy of your Facebook data," enter your password, and you will eventually be sent a link with the archive of your Facebook. Similarly, one can get their Twitter archive.

Miskel, *supra*.

How to Authenticate Social Media Evidence

"To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). "The [authentication] rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification. The rest is up to the jury." *United States v. Farrad*, 895 F.3d 859, 876 (6th Cir. 2018). In other words, evidence is authenticated under Rule 901 when evidence offered provides a "foundation from which the jury could reasonably find that the evidence is what the proponent says it is." *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE*, 2017 WL 5895911.

A court needs to find that sufficient evidence is present for the jury to conclude that the evidence is what the proponent of the evidence claims. *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (citations omitted). This provides a two-step process for authenticating social media evidence under Rule 901. *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra*. First, a court must determine whether the plaintiff has offered a satisfactory foundation. *United States v. Branch*, 970 F.2d 1368, 1370 (4th Cir. 1992). Second, if the plaintiff satisfies the first prong, the court will allow the jury to evaluate the surrounding evidence and determine the social media evidence is authentic. *Id*. at 1370-71.

Rule 901(b) contains a non-exhaustive list that satisfies the authentication requirement of Rule 901(a). For authenticating social media evidence, Rule 901(b)(1) and Rule 901(b)(4) are the most helpful. First, Rule 901(b)(1) permits authentication through the "testimony [of a witness with knowledge] that [the evidence] is what it is claimed to be." Fed. R. Evid. 901(b)(1). For electronic evidence, the witness testifying may be the person who created the electronic document or maintains the evidence in its electronic form. VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra. Therefore, for instance, an electronic communication--including an e-mail, text message, or a social media message--can be authenticated through the author's testimony, stating that he or she drafted or sent the communication. *See United States v. Barlow*, 568 F.3d 215, 220 (5th Cir. 2009) (holding that a chat log was properly authenticated by the testimony of a witness who participated in, and thus created, the chat). *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra*. Additionally, a recipient of the communication may also authenticate the message. *Id*. *See Talada v. City of Martinez*, 656 F. Supp. 2d 1147, 1158 (N.D. Cal. 2009) (holding that emails received were properly authenticated when the recipient provided a declaration asserting that the emails were true and correct copies).

The second method to authenticate social media evidence is through circumstantial evidence. Rule 901(b)(4) permits a party to authenticate evidence using circumstantial evidence with "the appearance, contents, substance, internal patterns, or other distinctive characteristics of the [evidence], taken together with all the

circumstances." Fed. R. Evid. 901(b)(4). "For example, where a witness testifies that an email or text message originated from the known e-mail address or screen name of another person, courts will generally find that the email or text message is an authentic communication from the purported sender." *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra*. In *People v. Pierre*, the court held that an instant message was properly authenticated when "[t]he accomplice witness . . . testified to defendant's [instant messenger] screen name. *People v. Pierre*, 838 N.Y.S.2d 546, 548-49 (2007). "[Another witness] testified that she sent an instant message to that same screen name, and received a reply, the content of which made no sense unless it was sent by defendant [and] there was no evidence that anyone had a motive, or opportunity, to impersonate defendant by using his screen name." *Id*. at 549.

How to Ensure that Social Media Evidence is Admissible

Whether Social Media Evidence is Improper Character Evidence

Under Rule 404(a) Federal Rules of Evidence states that "[e]vidence of a person's character or character trait is not admissible to prove that on a particular occasion that person acted in accordance with the character or trait." Fed. R. Evid. 404(a)(1). The rule also prohibits "[e]vidence of a crime, wrong, or other act . . . to prove a persons' character in order to show that on a particular occasion the person acted in accordance with the character." *Id*. at 404(b)(1). However, the propensity rule permits evidence admitted for another purpose, "such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident." *Id*. at 404(b)(2).

Courts have recently applied Rule 404 to social media evidence. For example, in *United States v. Phaknikone*, the government charged a defendant with robbing seven banks at gunpoint with the assistance of several accomplices. 605 F.3d 1099, 1103 (11th Cir. 2010). At trial, the prosecution argued that all the bank robberies shared signature traits, a modus operandi, that linked them to the same robber. *Id*. The prosecution then argued that "one of the signature traits of the common culprit in all seven robberies was to rob the banks like a gangster," which included holding a handgun "gangster-style." *Id*. To prove he robbed a strong of banks "like a gangster," the prosecution provided evidence from the defendant's social media page such as the profile page, subscriber report, and photographs. *Id*. at 1101.

On appeal, the 11th U.S. Circuit Court of Appeals addressed whether the district court abused its discretion by admitting the MySpace evidence to prove that the defendant committed a string of bank robberies "like a gangster." *Id*. As a result, the court set out a three-part test, analyzing: (1) whether the evidence is relevant to an issue other than the defendant's character; (2) whether there is sufficient proof so that a jury could find that the defendant committed the extrinsic act; and (3) whether the probative value of the evidence is substantially outweighed by its undue prejudice. *Id*. at 1107-08. The court applied this test "whenever the extrinsic activity reflects adversely on the character of the defendant, regardless of whether that activity might give rise to criminal liability." *Id*.

The MySpace evidence failed the first part of the test. The MySpace evidence offered to prove identity under Rule 404(b), and the evidence failed to show the required "'signature' crime" such that "the defendant must have used a modus operandi that is uniquely his." *Id*. at 1108. The court stated, "Evidence cannot be used to prove identity simply because the defendant has at other times committed the same commonplace variety of criminal act." *Id*. The court reasoned that "[a]lthough the photograph may portray a 'gangster-type personality,' the photograph does not evidence the modus operandi of a bank robber who commits his crimes with a signature trait." Id. at 1108-09. The court concluded that the MySpace evidence was "classic evidence of bad character," where the government tried to prove that the MySpace evidence was in conformity with an alleged propensity to commit the robberies in question. *Id*.

"It may be an effective strategy for counsel to display to the jury unflattering photographs or statements from an adverse party's social media profile. These images have a strong likelihood of damaging the party's image and creditability. To survive a Rule 404 challenge when applying this strategy, it is important that counsel find an applicable exception in Rule 404(b), such as motive, intent, or identity. Even then, a Rule 403 'unduly prejudicial' objection may keep the photos or statements out of evidence." *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra*.

Whether Social Media Evidence is Inadmissible Hearsay

Hearsay "means a statement that: a party offers in evidence to prove the truth of the matter asserted in the statement." Fed. R. Evid. 801(c). "Most of the information attorneys will seek to admit from social media websites (other than photographs) will qualify as 'out- of-court' statements potentially subject to the hearsay rule. However, because these statements are typically admissions by a party opponent, are not offered for their truth, or fall within a hearsay exception, they are typically not excluded under the hearsay rule." *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra. See United States v. Escobar*, 674 F.2d 469, 473-75 (5th Cir. 1982) (holding that the admission of a police officer's testimony when the computer printout showed the defendant as a "suspected narcotics smuggler" was hearsay).

Social Media Statements as Admissions by a Party Opponent

The Federal Rules of Evidence provide that a statement is not hearsay if it is a party's statement offered against that party, in either an individual or representative capacity. Fed. R. Evid. 801(d)(2). A party cannot offer its own out-of-court statements as admissions. VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra. "Given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party." *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 564-65 (D.MD. 2007) (citations omitted); *see also United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000) (holding that the email authored by the defendant was not hearsay because it was an admission by a party opponent); *United States v. Safavian*, 435 F.Supp.2d 36, 43 (D.D.C. 2006) (holding that the email sent by the defendant was admissible as non-hearsay because it constituted an admission by a party opponent).

Social Media Statements Offered for a Non-Hearsay Purpose

Even if a statement from a social media website is not an admission by a party opponent, it may very well be admissible because it is not offered for the truth of the matter asserted, and thus, not considered hearsay. Social media evidence is often admitted to prove something other than the truth of the statements contained therein. Examples of when statements may be relevant for some purpose other than to prove the truth of the matter asserted include: "those offered to prove the communicative or comprehensive capacity of the declarant; those offered as circumstantial evidence of the state of mind of the declarant; those offered to show the conduct of someone who heard them (to prove that they had knowledge of the information, or to explain what they did after having heard it); statements that constitute 'verbal acts' or parts of acts; and statements that have relevance even if not true." *See generally Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 565-67 (D.MD. 2007); *see also United States v. Hanson*, 994 F.2d 403, 406 (7th Cir. 1993) ("An out of court statement that is offered to show its effect on the hearer's state of mind is not hearsay."). Similarly, courts will admit statements from social media websites for impeachment purposes as prior inconsistent statements. *See e.g., In re K.W.*, 666 S.E.2d 490, 494 (2008) (holding that a victim's statements on her MySpace profile were admissible as prior inconsistent statements to impeach her testimony and should have been admitted by the trial court)." *VI. THE HURDLES TO ADMITTING SOCIAL MEDIA EVIDENCE, supra.*

Social Media Evidence Falling Within Hearsay Exceptions

Several hearsay exceptions are particularly relevant to social media evidence. Most relevant are the "present sense impression," "then existing mental, emotional, or physical condition," and "excited utterance" exceptions for social media evidence:

> The following are not excluded by the rule against hearsay, regardless of whether the declarant is available as a witness:
>
> (1) Present Sense Impression. A statement describing or explaining an event or condition, made while or immediately after the declarant perceived it.
>
> (2) Excited Utterance. A statement relating to a startling event or condition, made while the declarant was under the stress of excitement that it caused.
>
> (3) Then-Existing Mental, Emotional, or Physical Condition. A statement of the declarant's then-existing state of mind (such as motive, intent, or plan) or emotional, sensory, or physical condition (such as mental feeling, pain, or bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the validity or terms of the declarant's will.

Fed. R. Evid. 803(1)-(3). *See, e.g., United States v. Ferber*, 966 F. Supp. 90 (D. Mass. 1997) (holding that an email from employee to boss about substance of telephone call with defendant in mail/wire fraud case qualified as a present sense expression under Fed. R. Evid. 803(1), but did not qualify as an excited utterance under Fed. R. Evid. 803(2), despite the language at the end of the e-mail "my mind is mush.").

DEFENSIVE DISCOVERY

Objections to Plaintiff's Discovery

Fishing Expedition

See discussion *supra*, Sec. II.A.2.

Must be Particular Enough

See discussion *supra*, Sec. II.A.3.

No Reasonable Expectation of Privacy

Generally, courts do not recognize a privacy argument in the discovery of social media. Thus, anything that the company posts (or its employees post on the company behalf) are typically "fair game." Users of social networking sites "logically lack a legitimate expectation of privacy in the materials intended for publication or public postings." *Guest v. Leis*, 225 F.3d 325, 333 (6th Cir. 2011). "[T]he act of posting information on a social networking site, without the post limiting access to that information, makes whatever is posted available to the word at large." Indp. Newspapers, Inc. v. Brodie, 966 A.2d 432,

438 (Md. 2009). "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." *Romano v Steelcase Inc.*, 907 N.Y.S. 2d 650, 657 (2010).

Arguing Against Authentication/Admissibility of Client's Social Media

Authentication

Three potential challenges exist to the authentication of a client's social media. The first is when the proponent fails to satisfy the preponderance of evidence standard for authentication. The second is that authentication of ESI can be manipulated or corrupted. *United States v. Browne,* 834 F.3d 403, 437 (3rd Cir. 2016) (citing (*Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007)). The third is that the authentication of social media evidence presents some special challenges because of the great ease with which a social media account may be falsified, or a legitimate account may be accessed by an imposter. *Id*. at 437-48 (citing Cf. *Griffin v. State*, 19 A.3d 415, 424 (2011) (analyzing state analogue to Rule 901)).

For example, the court in Griffin v. State concluded that the trial court wrongly found that MySpace evidence was properly authenticated: "We agree with [the defendant] that the trial judge abused his discretion in admitting the MySpace evidence pursuant to Rule 5– 901(b)(4), because the picture of [the defendant's girlfriend], coupled with her birth date and location, were not sufficient 'distinctive characteristics' on a MySpace profile to authenticate its printout, given the prospect that someone other than [the defendant's girlfriend] could have not only created the site, but also posted the 'snitches get stitches' comment." 19 A.3d 415, 423-24 (2011). The court noted the potential for manipulation of a social networking site where a printed image from a site "requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that [the defendant's girlfriend] was its creator and the author of the 'snitches get stitches' language." *Id*. at 424.

In Lorraine v. Markel American Ins. Co., the court cited numerous examples where proponents of ESI failed to properly authenticate it. *See Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 542 (D. Md. 2007) citing (see, e.g., *In re Vee Vinhnee*, 336 B.R. 437 (proponent failed to properly authenticate exhibits of electronically stored business records); *United States v. Jackson,* 208 F.3d 633, 638 (7th Cir.2000) (proponent failed to authenticate exhibits taken from an organization's website); *St. Luke's Cataract and Laser Institute PA v. Sanderson*, 2006 WL 1320242, at *3–4 (M.D. Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Rambus v. Infineon Tech. AG*, 348 F.Supp.2d 698 (E.D.Va.2004) (proponent failed to authenticate computer generated business records); *Wady v. Provident Life and Accident Ins. Co. of Am.*, 216 F.Supp.2d 1060 (C.D.Cal.2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge)*; Indianapolis Minority Contractors Assoc., Inc. v. Wiley*, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them)).

Also, the *Lorraine* court cited one commentator of the Federal Rules of Evidence who expressed concern of authenticating electronic documents:

> In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting but can also happen when

> defective software programs are used or stored-data media become corrupted or damaged.

Id. at 543.

Character Evidence

A lot of social media evidence can often be considered inadmissible character evidence. Fed. R. Evid. 404(a). For example, "[t]he compromising photograph or the kiss with the paramour is sometimes admissible only to suggest that the witness has bad character. Do not let your opponent get away with admitting a compromising photograph just because he can. If you cannot keep out the evidence all together, at least slow down his or her momentum and make the opponent offer the bad evidence against your client for a limited purpose. [Fed. R. Evid.] 404(b)." Bill Henry et al., *XX. YOUR OPPONENT SPRINGS A SOCIAL MEDIA TRAP ON YOU*, 2018 TXCLE-AFL 56-XX, 2018 WL 6366749 (2018).

Irrelevant (Waste of Time)

Some social media evidence is completely irrelevant to the present matter. The social media evidence presented must should make a consequential fact more or less probable, Fed. R. Evid. 401, and the probative value cannot be substantially outweighed by the danger of unfair prejudice or concerns of misleading the jury, Fed. R. Evid. 403. "Keep in mind that something can be relevant if used for impeachment purposes. Be sure to remember that the item is inadmissible if its probative value is substantially outweighed by the danger of confusion of the issues. One way to keep explosive documents out of evidence is to let the trial court know that the admission of the damaging pictures [opens] a whole new line of inquiry that will take the trial in a new direction and will substantially increase the length of the trial. On a close question of relevancy, you can keep out evidence if the trial court is convinced that it will add hours of additional time to the trial." Henry, *supra*.

Hearsay – Offered to Prove the Truth of the Matter Asserted

"If a statement implies a fact, it is still hearsay. Even if a statement does not directly state a fact it is still hearsay. The reason is that a 'matter asserted' is any matter explicitly asserted or any matter implied by a statement if it stems from the third-party declarant's belief about the matter. Fed. R. Evid. 801(c). The classic example is a third-party caller who calls a telephone number and says, 'Put 10 dollars down on the old mare in the tenth race.' Although the statement itself is not a direct statement of fact, it implies the fact that the owner of the telephone number is taking bets and the caller believes that fact. Because it is being offered as an implied fact, it is a matter asserted under Fed. R. Evid. 801 and is hearsay. Often in trial we will get caught up in the argument that the statement is not the 'truth of the matter asserted' and will let implied hearsay statements get into evidence." Henry, *supra*.

The excited utterance exception is a relatively broad exception that can be used to admit social media evidence. "The exciting event can occur, then a relatively long period of time can elapse, then the statement can be made that falls within the excited utterance exception." *Id*.

In addition, an emoji or emoticon may be hearsay because it can be a nonverbal statement that is intended as a substitute for a verbal statement. *Id*.

CONCLUSION

The use of social media in litigation is an ever-evolving area of the law and attorneys must be diligent in understanding the ins and outs of what it is, how to get it, how to use it, and how to defend against it. Hopefully this article provided insight on just that #stayinformed.