Social Media Evidence: Ethical and Practical Considerations for Collecting and Using Social Media Evidence in Litigation

Sean O'D. Bosack
Daniel J. Blinka
Godfrey & Kahn, S.C.
Milwaukee, Wisconsin

Laura A. Brenner
Kate E. Maternowski
Reinhart, Boerner, Van Deuren, s.c.
Milwaukee, Wisconsin

I. INTRODUCTION

"Social Media" has revolutionized the nature and speed of human interaction. Instead of speaking in person or on the phone, or writing a letter, many people "post" on Facebook, Instagram, or Pinterest, or send text messages or "tweets." In the not-so-distant past, communications could be easily discarded, and difficult to reconstruct as memories faded. Communications through social media, however, are more likely to be preserved, and easily retrieved.

Today, infinitely more information is available that may shed light on the nature of a promise, a party's intention or motive, or otherwise serve as evidence that conduct did or did not occur. Technology also allows false evidence to be easily manufactured, and communications that may have been intended to be private may actually be accessible to people who were not the intended recipients. These new modes of communication have changed the face of litigation. In-house and outside counsel must understand the universe of potentially available social media in order to effectively mount fact investigations and prosecute and defend claims on behalf of their clients. Moreover, it is equally important that in-house and outside counsel consider

ethical, procedural and practical challenges unique to the collection and use of social media evidence.

This article first discusses types and sources of information available, and addresses unique ethical issues that arise during the process of gathering such evidence. Next, it addresses discovery of social media evidence in civil discovery. Finally, we evaluate the admissibility of social media evidence in court.

II. SOURCES OF SOCIAL MEDIA EVIDENCE

Before examining unique issues surrounding the acquisition and admissibility of social media evidence, it is necessary to understand the universe of social media evidence available. While some of the most popular social media outlets, such as Facebook, Twitter, and LinkedIn, have become household names, there is a vast universe of social media about which in-house and outside counsel alike should develop a baseline knowledge.

Social Networks (Facebook, LinkedIn, and Match.com): These services typically consist of a user profile, various ways to interact with other users both privately and publicly, and the ability to organize groups and events.

Media Sharing (YouTube, Instagram, Pinterest, and Flickr): These services allow users to upload and share various media such as photos and video and usually also include user profile and commenting features.

Activity Tracking (Nike + Running, FourSquare, and GHIN.com): These services allow users to record and broadcast certain activities, such as running a certain distance or visiting a certain restaurant.

Blogs and Microblogs (WordPress and Twitter): Blogs are individual user websites that function like diaries, and microblogs are similar platforms that focus on short updates pushed out to anyone subscribed to receive them.

Social News (Digg and Reddit): These services allow users to share news items or links to news articles and vote and comment on those posts.

Discussion Forums: These are places for online communities to discuss topics of common interest.

Comments and Reviews (TripAdvisor and Yelp): In addition to the platforms listed above, user content abounds in the comment sections of travel websites, newspaper sites, and so on.

These categories of social media often overlap and are certainly not exhaustive. An effective investigation of online user data will mine information from all of these categories. [1]

III. ACQUIRING CONTENT

Social media evidence can be acquired both informally – often as part of an investigation conducted by an in-house legal or human resources department in order to determine whether some form of employee misconduct occurred – or more formally through discovery under rules of civil procedure in litigation. Each gives rise to different practical and ethical issues. On one hand, informal investigations delving into social media outlets used by company employees and potential adversaries spawn a wide variety of ethical and privacy issues. On the other, formal discovery once litigation has commenced gives rise to more practical and procedural issues.

[1] For an in-depth tutorial on searching the Internet's most popular social media networks, *see* Thomas Roe Frazer II, *Social Media: From Discovery to Marketing - A Primer for Lawyers*, 36 AM. J. TRIAL ADVOC. 539, 559-64 (2013).

A. Informal Investigation

Management may have reported to in-house counsel that it believes a key employee has been planning his or her departure from the company to join a competitor, or otherwise engaged in misconduct. In-house counsel may recommend that the company conduct an internal investigation to determine whether the report is true, whether the employee has misappropriated trade secrets, and whether the company may have a claim against its competitor.

Analysis of social media outlets that the employee may have used can, and should, be part of the investigation. Most social media networks allow users to decide through privacy settings which of their data is available to whom, but many users choose to broadcast a significant amount of data to the general public. State bar committees examining this issue generally agree that a lawyer's investigation of publically available data is ethical.[2] Acquiring evidence in violation of the law or lawyer ethics rules, however, could compromise the admissibility of the evidence, or subject the lawyer to discipline or even criminal liability. Some pitfalls unique to social media analysis and practical solutions are discussed below.

1. Pretexting.

Pretexting generally involves misrepresenting one's identity to another for the purpose of obtaining information. In the social media context, pretexting consists of, for example, using a false identity to send a "friend" request to an adverse witness on Facebook for the purpose of obtaining impeachment evidence. Generally speaking, sending a friend request to an unrepresented person without making attempts to mislead that person about the requestor's identity or motive is ethically in-bounds.[3] More creative deceptive tactics, however, likely constitute violations of ethical rules or other laws.

---

[2] *See, e.g.,* N.Y. State Bar Ass'n, N.Y. Comm. on Prof'l Ethics, Op. 843 (Sept. 10, 2010) ("Obtaining information about a party available in the [public] 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 such as Nexis or Factiva, and that is plainly permitted.").

[3] *See, e.g.,* New York State Bar Ass'n, Formal Op. 843 (Sept. 10, 2010).

A lawyer who sends a misleading friend request—concealing or lying about her identity–likely violates American Bar Association Model Rules 4.1 and 8.4(c). Those rules prohibit lawyers from making false statements of material fact to a third person and from engaging in conduct that involves dishonesty, fraud, deceit, or misrepresentation. Instructing someone else, such as a private investigator or member of a corporate security department, to send the friend request is no better: Model Rule 8.4(a) prohibits lawyers from violating the rules themselves or through the actions of another.

Deceptive "friending" can even lead to misdemeanor charges for the requestor. For example, California law provides that an attorney who commits or consents to deceit or collusion with intent to deceive a party is guilty of a misdemeanor.[4] Additionally, in California, "any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person" can face a fine and even jail time.[5]

Finally, a lawyer's contact with a represented party, even through a non-deceptive Facebook request, violates ethical rules.[6] Because such a request is sent in order to obtain information for a lawsuit, it likely constitutes a communication "about the subject of the representation."[7]

2. Privacy Concerns.

Many social media sites provide users the option of adjusting privacy settings so as to allow only certain people or groups access to their content. But privacy objections are generally fruitless in defending against a discovery request for social media content, even if the user

[4] CAL. BUS. & PROF. CODE §6128(A).
[5] CAL. PENAL CODE §528.5.
[6] MODEL RULES OF PROF'L CONDUCT, R. 4.2; *see also* New York State Bar Ass'n, Formal Op. 843 (Sept. 10, 2010).
[7] *Id.; see also* San Diego County Bar Ass'n Legal Ethics Comm., Op. 2011-2 (May 24, 2011).

employs privacy settings.[8] State privacy laws, however, should give a lawyer pause before collecting online content informally.

For example, California recently enacted legislation that generally prohibits an employer from requesting or demanding an employee's password to or the contents of his personal social media accounts.[9] The law does have an exception for investigations of employee misconduct, but even in the context of an investigation an employer cannot request the employee's password—he can only request content relevant to the investigation.[10] California isn't alone: a majority of the states have either enacted similar laws or are considering pending legislation.[11]

3. Privacy and Social Media Policies.

A company or employer seeking some level of control over or access to employee social media should craft and enforce a privacy policy that puts employees on notice regarding online content for which they can reasonably expect privacy. Applicable privacy laws must be considered during drafting, along with other applicable laws and regulations governing privacy and individuals' right to freedom of speech.[12]

Whether an employer can access its employees' personal online data generally depends upon whether the employees have a reasonable expectation of privacy in that data. Most jurisdictions agree that an employee does not have a reasonable expectation of privacy in messages sent over a company account.[13] But when an employee sends messages on company equipment with a personal account, the answer isn't as clear. For example, in *Stengart v. Loving*

---

[8] *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010) ("[W]hen 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.").
[9] CAL. LABOR CODE § 980(b).
[10] *Id.* § 980(c).
[11] *See Employer Access to Social Media Usernames and Passwords*, NATIONAL CONFERENCE OF STATE LEGISLATURES (last modified Jan. 14, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2013.
[12] *See, e.g.*, NLRB, Operations Memorandum 12-59 (May 30, 2012) ("OM 12-59") (General Counsel of the National Labor Relations Board Memorandum providing enforcement guidance on employees' use of social media and employers' social media policies).
[13] *See, e.g., Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101, 64 USLW 2564, 131 Lab. Cas. (BNA) P 58104, 11 IER Cases 585 (E.D. Pa. 1996).

Care Agency, Inc., the New Jersey Supreme Court found that an employee had a reasonable expectation of privacy in emails she sent to her attorney from a personal account accessed on her company-issued laptop.[14] Although *Stengart* primarily dealt with issues of privilege, its analysis of employee privacy provides a good lesson for in-house counsel drafting privacy policies.

The *Stengart* court concluded that the employer's electronic communications policy was deficient because it failed to explicitly address personal email accounts, it failed to communicate to employees that emails from their personal accounts could be stored on a work computer's hard drive and later retrieved by the employer, and while the policy stated that "emails are not to be considered private or personal to any individual employee," it also permitted "[o]ccasional personal use [of email]."[15] The court held that an employee reading the policy could have a reasonable expectation in the privacy of personal email sent from work computers.[16] A more explicit privacy policy might have defeated the plaintiff employee's expectation of privacy.

Employers should also implement social media privacy policies that detail the ownership rights of employee social media content. To date, three courts have addressed the extent to which an employer can assert an interest in social media content on an employee's account.[17] Only two of those cases made definitive ruling regarding the rights of employer to claim trade secret protection over employee social media. In *Christou v. Beatport*, the court allowed an employer's trade secret misappropriation claim premised on the theft of MySpace friends to survive the pleading stage, while the court in *Eagle v. Morgan* found that LinkedIn contacts did not constitute a trade secret because information regarding the company's customers and connections was publicly available. The *Eagle* court did, however, find that the company could assert an ownership interest in its former executive's LinkedIn account that had been established

[14] 990 A.2d 650 (N.J. 2010).
[15] *Id*. at 659.
[16] *Id.* at 663.
[17] *PhoneDog v. Kravitz*, No. C11-03474 MEJ, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011); *Christou v. Beatport, LLC*, No. 10-cv-02912, 2012 WL 872574, RBJ-KMT, (D. Colo. March 14, 2012); *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011).

and maintained by the company and for the company's benefit. An explicit and clear social media policy would describe exactly which content belongs to the employer.

B. Formal Discovery

Although the universe of published case law concerning social media discovery disputes remains relatively undeveloped, decisions that have been published confirm at least this: social media data is fair game in formal discovery.

Privacy objections have by and large proven unsuccessful in preventing a party from obtaining another party's personal online data. In *Loporcaro v. City of New York*, for example, a New York trial court judge opined that:

> [w]hen a person creates a Facebook account, he or she may be found to have consented to the possibility that personal information might be shared with others, notwithstanding his or her privacy settings, as there is no guarantee that the pictures and information posted thereon, whether personal or not, will not be further broadcast and made available to other members of the public.[18]

Despite apparent unanimity among courts agreeing that litigants can seek social media evidence in discovery, there is not yet consistency in how evidence should be produced. The published opinions to date generally illustrate three approaches courts employ. Each places the burden of relevance review on a different player: the court itself, the producing party, or the requesting party.

1. Burden of Review on the Court.

This method is most unlike standard discovery practices and gives the court considerable control over the evidence available to the parties. Under this approach, the producing party is directed to give the judge access to the social media account subject to the request, and the judge then reviews the account in camera to determine discoverability. The judge can gain access to

[18] No. 100406/10, 2012 WL 1231021 (N.Y. Sup. Ct. April 9, 2012).

the producing party's social media account either by "friending" the party,[19] or requiring the party to turn over user names and passwords.[20]

This method of discovery sidesteps the concern that the producing party will under-produce in response to request for production of documents.[21] It also spares the parties from culling through mountains of material and fighting about relevance among themselves.[22]

2. Burden of Review on Producing Party.

Courts have directed the producing party to respond to a social media discovery request by developing search terms or other searching protocol to locate relevant information. The producing party, typically with assistance of counsel, reviews the collected material him- or herself to decide which data is responsive.

In *EEOC v. Simply Storage Management, LLC,* for example, the defendant employer sought access to the complainants' Facebook accounts to locate data concerning emotional damages.[23] The court opined that:

> [d]iscovery is intended to be a self-regulating process that depends on the reasonableness and cooperation of counsel. Here, in the first instance, the [claimants'] counsel will make those [relevancy] determinations based on the guidelines the court has provided. As with discovery generally, [the defendant] can further inquire of counsel and the claimants (in their depositions) about what has and has not been produced and can challenge the production if it believes the production falls short of the requirements of this order.[24]

This production method has benefits and drawbacks for both parties. On one hand, this method relieves the requesting party from the burden and expense of sifting through a potentially staggering amount of data and places that burden instead on the producing party. On the other

---

[19] *See, e.g., Barnes v. CUS Nashville, LLC*, 3:09-CV-00764, 2010 WL 2265668 (M.D. Tenn. June 3, 2010).
[20] *See, e.g., Offenback v. L.M. Bowman, Inc*., 1:10-CV-1789, 2011 WL 2491371 (M.D. Pa. June 22, 2011).
[21] *Bass ex rel. Bass v. Miss Porter's Sch.*, 3:08 CV 1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009) ("production should not be limited to Plaintiff's own determination of what may be 'reasonably calculated to lead to the discovery of admissible evidence.'").
[22] After doing the culling himself, one judge colorfully opined that the account revealed "little beyond routine communications with family and friends, an interest in bluegrass and country music, a photography hobby, sporadic observations about current events, and a passion for the Philadelphia Phillies that was not dampened after he moved to Kentucky from Pennsylvania." *Offenback*, 1:10-CV-1789, 2011 WL 2491371, at *3.
[23] 270 F.R.D. 430 (S.D. Ind. 2010).
[24] *Id*. at 436 (internal citation omitted).

hand, this method gives the producing party an opportunity to make the first decision about relevance, and the requesting party might suspect that the final production is not as thorough as it could be.

3. Burden of Review on the Requesting Party.

This method is largely considered the gold standard for requesting parties. Despite the possibility that it could result in significant expenditure of time and resources, requesting parties relish the opportunity to view a producing party's entire social media account and make their own relevancy determinations. Courts that allow this method of discovery typically require a preliminary showing of relevance in the public portions of the social media account before the requesting party is given full access either by provision of usernames and passwords or consent to the social media company to release the user data.[25]

But courts and, to an even greater extent, producing parties are often resistant to the allowance of unfettered access by one party to another party's entire social media account.[26] Courts often deny a requesting party this type of unfettered access, reasoning that the requesting party has not made an adequate showing of relevance and is not entitled to embark on a fishing expedition to dig up something relevant.[27]

Against this backdrop, the following serve as some practical tips that may help attorneys efficiently and effectively gain access to useful social media information through civil discovery.

---

[25] *See, e.g., Largent v. Reed*, No. 2009-1823, 2011 WL 5632688 (Pa. Com. Pl. Nov. 8, 2011) (requiring plaintiff to turn over username and password and allotting defense counsel 21 days to inspect the plaintiff's profile, after which the plaintiff could change her password); *Al Noaimi v. Zaid*, No. 11-1156-EFM, 2012 WL 4758048 (D. Kan. Oct. 5, 2012) (ordering the producing party to execute a consent that would allow social media site to produce content directly to the requesting party).

[26] It bears mention a Facebook user's turning over of his account information to a third party for inspection of the account data actually violates the site's Terms of Service, Statement of Rights and Responsibilities, Facebook (last modified November 15, 2013), https://www.facebook.com/legal/terms ("You will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.").

[27] *Salvato v. Miley*, No. 5:12-CV-635-OC-10PRL, 2013 WL 2712206 (M.D. Fla. June 11, 2013) ("The party seeking discovery has the threshold burden of showing that the requested discovery is relevant.").

1. Carefully Tailor Discovery Requests.

Despite a clear trend by courts to allow at least some form of discovery of social media evidence, this type of evidentiary search has its limits. The primary reason courts deny a litigant's request to compel production of social media evidence is that the request is overbroad.

So-called "fishing expeditions" have been frowned on long before the arrival of social media, but curry even greater disfavor as technology advances.[28] Courts do not ease standards on overly broad and vague requests simply because the data sought is electronic and therefore easier to gather. Given the wide range of information available on a user's social media page or account, a discovery request that is drafted without particularity—asking for all information posted to social media, for example—will likely be subject to an objection that is it overbroad and unduly burdensome.

In a recent medical malpractice case in the District of Maryland, the defendants moved to compel discovery from both the plaintiff and the plaintiff's expert of "'any documents [,] postings, pictures, messages[,] or entries of any kind on social media within the covered period relating to [c]laims by Plaintiffs or their [e]xperts.'"[29] The court denied the request to compel, holding that the request was "not narrowly tailored" and "does not describe the categories of material sought; rather, it relies on Plaintiffs to determine what might be relevant."[30]

Therefore, counsel should be careful to draft discovery requests with particularity when seeking to obtain social media evidence. All requests should demonstrably relate to facts of the case and impose as little a burden as possible on the producing party, especially if the producing party is tasked with reviewing its own material for relevance.

---

[28] *Caraballo v. City of New York*, No. 103477/08, 2001 N.Y. Slip Op. 30605LU), 2011 WL 972547 (N.Y. Sup. Ct. Mar. 4, 2011) ("digital 'fishing expeditions' are no less objectionable than their analog antecedents").
[29] *Ford v. United States*, CIV.A. DKC11-3039, 2013 WL 3877756, at *1 (D. Md. July 25, 2013).
[30] *Id.* at *2.

2. Beware of Spoliation.

As with all evidence, parties may not conceal or destroy social media evidence. In *Lester v. Allied Concrete Co*., the actions of the plaintiff and his attorney in response to a social media discovery request resulted in the Virginia Circuit Court of the City of Charlottesville imposing substantial monetary sanctions against both the plaintiff and his attorney.[31]

The plaintiff in *Lester* requested screen print outs of Lester's Facebook account. In response, Plaintiff's attorney advised him to "clean up" his Facebook because "we don't want blowups of this stuff at trial."[32] Defense counsel filed a motion to compel discovery and Lester's attorney instructed him to reactivate the account but to delete several photos. These facts came to light because the defendant hired a computer expert to examine IP logs from Facebook, which revealed that Lester had deleted 16 photographs. The court ordered plaintiff and his attorney to pay reasonable expenses, including attorney fees totaling $722,000.00, and referred ethics-based allegations against counsel to the Virginia State Bar.[33]

This case also highlights the fact that not all that appears to be deleted is lost. For example, if an active account disappears from Facebook, it is possible the user "deactivated" his account without deleting it altogether. A deactivated account is suspended and unsearchable but can be reactivated at the election of the user.[34] In contrast, a deleted Facebook account is likely gone permanently, meaning that all information previously contained in the account is deleted except for "[c]opies of some material (photos, notes, etc.) may remain in our servers for technical reasons."[35]

---

[31] Nos. CL.08-150, CL09-223 (Va. Cir. Ct. Sept. 1, 2011).
[32] *Id.*
[33] *Id.*
[34] *Deactivating, Deleting & Memorializing Accounts*, Facebook (last modified Jan. 7, 2014), available at https://www.facebook.com/help/359046244166395.
[35] *Id.*

3. Consider the Applicability of the Stored Communications Act

Given the potential complications of requesting social media content in formal discovery, an attorney might be tempted to skip the interrogatories and request the data from the social media outlets directly. One major hurdle, though, stands in the way of success with this approach: the Stored Communications Act ("SCA").[36] The SCA generally prohibits any entity that provides electronic communication services ("ECS") or remote computing services ("RCS") from disclosing the contents of its users' communications to non-government entities without user consent.[37] In other words, the SCA shields from civil subpoenas providers and networks that send and store electronic communications for their users.[38]

Courts have held that certain online entities such as Yahoo!, Google, AOL, and YouTube are governed by the SCA, but very few courts have examined whether social media outlets fall within the SCA's ambit. What little guidance is available suggests they do. For example, in *Crispin v. Christian Audigier, Inc.*, the court held that so long as a Facebook user has some privacy setting in place such that his profile is not entirely available to the general public, the SCA will prohibit Facebook from producing user content without his consent.[39] Accordingly, civil litigants should not rely exclusively on third-party subpoenas to social media providers; the better approach is to request social media data in formal discovery, as described above.

IV. ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE

Like any documentary evidence, social media evidence is admissible only if relevant, authenticated, and, in most circumstances, overcomes hearsay rules. While the rules

[36] 18 U.S.C §§ 2701-2711 (enacted as Title II of the Electronic Communications Privacy Act).
[37] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C § 2510(15). An RCS is a service that provides "computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).
[38] The SCA does provide numerous exceptions for government access to user data without user consent, outlined in 18 U.S.C. § 2703.
[39] 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010); *but see Juror No. One v. Superior Court*, 142 Cal. Rptr. 3d 151, 158 (Cal. Ct. App. 2012) ("Assuming *Crispin* was correctly decided, that case did not establish *as a matter of law* that Facebook is either an ECS or an RCS or that the postings to that service are protected by the SCA.") (emphasis in original).

of evidence (Federal and most states) do not specifically address admissibility and authentication of electronically stored evidence, the rules do not treat electronically stored information, or social media evidence, differently from any other type of evidence. As such, the Rules of Evidence form the framework for considering admissibility and authenticity.

Generally, the rules provide no significant bar to admissibility of relevant social media evidence. There are, however, practical complications unique to social media evidence. Authentication is usually the most significant hurdle to be overcome. In addition, the proponent of social media evidence may face challenges to overcome the hearsay rule.

A. Authentication

Authentication is governed by Federal Rule of Evidence 901, and in many instances circumstantial evidence may be the key to successful authentication of social media evidence. Authentication is the identification of evidence. Authentication and identification are "special aspects" of relevancy.[40] In order to authenticate evidence, the proponent of the evidence must offer sufficient evidence "that the matter in question is what the proponent claims."

Federal Rule of Evidence 901(b) outlines examples of evidence that satisfy the general requirement of authentication. Rule 901(b) is illustrative. Because 901(b) merely sets forth examples, rather than rules, it need not be rigidly or technically applied.[41] A handful of Rule 901(b) examples are applicable to social media evidence.

1. Testimony of a Witness With Knowledge.

A social media webpage or web-posting may be authenticated or identified through testimony of a witness with knowledge that the "matter is what it is claimed to be."[42] The owner of the Facebook page may identify it as his page, and further identify the statement in issue as his

[40] FED. R. EVID. 901(1), advisory committee's note ("Authentication and identification represent a special aspect of relevancy.)"
[41] FED R. EVID. 901(b), advisory. Rule 901(b) provides examples, not "rules," which are intended only to "guide and suggest" determinations under 901(b).
[42] FED R. EVID. 901(b)(1).

post or comment. Therefore, in a civil lawsuit, the proponent may serve a request for admission prior to moving for summary judgment in order to authenticate the Facebook post. Alternatively, the proponent may also be able to authenticate the Facebook post through a witness who watched the defendant submit his or her post. Similarly, photographs may be authenticated by any witness who can testify that they fairly and accurately depict things of which the witness has personal knowledge. The same may be true for a text entry, such as comment or post. Testimony by the person who took the pictures or wrote the post may achieve authentication.

When offering a print-out of a Facebook page, the print-out can be authenticated by a witness who can testify that she went to the website using the assigned URL, viewed the information, and that the print-out fairly and accurately represents what she saw at the website.[43] With that being said, concerns that the witness, or another, may have altered the information, or that a third party may have inserted erroneous information on the website, may raise questions of credibility or, in very extreme circumstances, lead to exclusion under Rule 403.

2. Comparison By Trier or Expert Witness.

Comparisons by both expert witnesses and the trier of fact itself are permitted.[44] The expert or the trier of fact compares "known" examples (the defendant's Facebook page for example) with the questioned evidence (a printout of the defendant's Facebook page from another day) in order to determine if they came from the same source. The trier of fact may conclude that the Facebook page in question features the same profile picture or biographical information as an already authenticated but different print-out from the defendant's Facebook page. In order for the evidence to be admissible, the trier of fact must be able to determine with a reasonable degree of certainty that the evidence comes from the same source as the previously authenticated comparison.

[43] *See ACTONet, Ltd. v. Allou Health & Beauty Care*, 219 F.3d 836, 848 (8th Cir. 2000).
[44] FED. R. EVID. 901(b)(3).

3. Distinctive Characteristics.

Identification or authentication may be circumstantially established through an item's appearance, content, substance, internal patterns or other distinctive characteristics.[45] For example, the post in question may contain a unique signature or sign-off. Similarly, the repeated misspellings of certain words may provide a sufficient link between the questioned document and the known works of a poor speller to support the inference that he or she authored the document.[46]

In a recent criminal case, a court admitted a MySpace profile into evidence based upon circumstantial evidence.[47] The MySpace profile contained numerous photographs of the defendant. The profile referenced the death of the victim and the music played at the victim's funeral. It further referenced the defendant's gang. Perhaps most important, the author's name corresponded with the defendant's name and nickname, as did the author's email address. Based upon the foregoing, the court determined there was a sufficient showing that the MySpace profile was authored by the defendant.

Another recent decision, however, illustrates courts' uneasiness with authenticating social media evidence based solely upon circumstantial evidence.[48] *Griffin v. State* determined the proponent of the evidence could not establish the author of a MySpace post based solely on a photo, a location, and a date of birth. The court was wary of the fact that someone else could have posted the comments. The court went on to state that "authenticating electronically stored information presents a myriad of concerns because 'technology changes so rapidly' and is 'often new to many judges.'"[49] It, therefore, "requires greater scrutiny of 'the foundational

---

[45] FED. R. EVID. 901(b)(4).
[46] *United States v. Clifford*, 704 F.2d 86, 90-91 (3d Cir. 1983) (Weinstein notes that "the technique [of identifying a writer by the internal patterns of the writing]—without the aid of experts or computers—is one long used in the courts.") (internal citations omitted).
[47] *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012).
[48] *Griffin v. State*, 19 A.3d 415 (Md. Apr. 2011)).
[49] *Id*. at 423.

requirements' than letters or other paper records, to bolster reliability.'"[50] The court was particularly concerned with the premise that the profile may not be legitimate because it is relatively easy to create a fictitious account.[51] *Griffin* presents an important lesson: gather as much circumstantial evidence as possible before you present evidence from any social media site, or any website.

There are other ways to authenticate information form social media. Ultimately, the proponent must present sufficient evidence to establish that the social media or website post or comments are what the proponent says they are. Before offering any social media evidence, the proponent should be able to answer the following questions: (1) How was the evidence created? (2) How and where was the evidence collected? (3) What types of evidence were collected? (4) When was the evidence collected?[52]

When offering a post, entry or other writing set forth on a social media website against someone, the proponent should first determine whether the Facebook, MySpace, and other social media site can only be accessed by the owner of the account, armed with his or her username and password. Second, the proponent should consider locating profile pictures or other information unique to the individual alleged to have written the Facebook post or blog entry. The content of the Facebook page itself may provide sufficient evidence of authenticity. Third, metadata associated with the website from which the social media evidence was obtained may reveal evidence of the date, time and author of the posting. Fourth, if the social media evidence is obtained from an individual's personal or work computer—a computer to which only that individual had access—that too may be sufficient circumstantial evidence of the fact that the individual the proponent claims made the posting actually made the posting. For example, where a defamatory posting is made on an employee's Facebook page, the post is time stamped 9:00

[50] *Id*.
[51] *Id*. at 421-22.
[52] Gilliland, Josh, *The Admissibility of Social Media Evidence*, LITIGATION, Vol. 39, No. 1, Winter 2013.

a.m. on June 1, 2012, and the same individual's browser history (which he or she forgot to delete) reveals a trip to Facebook at 9:00 a.m. on June 1, 2012, the chain of evidence may be sufficient to authenticate the Facebook posting as that of the employee in question.

The more circumstantial evidence the proponent can offer to support the proposition that the social media post is authentic, the more likely a court will allow it into evidence.

B. Hearsay Rules

More often than not, the proponent of social media evidence (at least posts or comments) offers the statement made by a declarant for the truth of the matter asserted.[53] Therefore, the proponent must be prepared to establish that the social media evidence falls under a hearsay exception or is exempt from the rule against hearsay.[54] There are no special applications of the hearsay exceptions unique to social media.

Sometimes, an opposing party's statement may be exempt from the hearsay rule. If evidence of a Facebook or other web-posting by your adversary is properly authenticated and offered against the adversary, then the statement is exempt from the hearsay rule as an opposing party statement.[55] For example, in *B.M. v. D.M.*, a divorce proceeding in which the wife sought non-durational maintenance alleging she could not work due to a physical injury, her husband was allowed to use authenticated posts made by the wife on a website against the wife.[56] The posts indicated that she could in fact work and was capable of traveling, which was contrary to her testimony.[57]

In addition, the rules of evidence allow admission of out-of-court statements when the statement is consistent with the declarant's testimony and is offered to rebut an express or implied charge that the declarant recently fabricated it or acted from a recent improper influence

[53] With respect to photos, there is no statement. Therefore, the hearsay rule does not apply.
[54] *See generally*, FED. R. EVID. 801 and 803.
[55] FED. R. EVID. 801(d)(2).
[56] *B.M. v. D.M.*, No. 50333/2007, 2011 WL 1420917 (N.Y. Sup. Ct. Apr. 7, 2011).
[57] *Id*.

or motive in so testifying.[58] The proponent of the evidence might use a Facebook post to rehabilitate a witness that has been impeached.

Other statements may qualify as exceptions to the rule against hearsay. It may be possible for a Facebook post to be admitted into evidence as a present sense impression, excited utterance, or then-existing mental, emotional or physical condition. A plaintiff in a personal injury case may have written posts on his or her Facebook page stating that he or she cannot believe she ran a red light. Counsel must be prepared to lay a foundation for the present sense impression, or other exception to the rule against hearsay.

C. Illegally Obtained Evidence

As discussed previously, it may be tempting for both in-house and outside counsel to employ stealthy or clandestine means to acquire evidence through social media outlets. Perhaps in-house counsel hired a private investigator to snoop for evidence of employee misconduct, and believes he may find incriminating evidence on the employee's Facebook page. In order to view the page, he issues a friend request, pretending to be a known friend of the employee, and when he accesses the employee's Facebook page, he finds incriminating evidence. In-house counsel then provides the evidence to the company's outside counsel and explains every detail of the investigator's efforts to acquire the evidence.

In civil litigation, the evidence may very well be admissible even though it was obtained unethically. Many courts have held that the admissibility of evidence is not affected by the means through which it is obtained.[59] Absent some constitutional, statutory, or decisional authority mandating the suppression of otherwise valid evidence, such evidence will be

[58] FED. R. EVID. 801(d)(1)(B).
[59] *See e.g. Stagg v. New York City Health & Hospitals Corp.*, 556 N.Y.S.2d 779 (App. Div. 1990); *United States v. Janis*, 428 U.S. 433, 454 (the exclusionary rule does not apply to civil claims brought by the IRS).

admissible even if procured by unethical or unlawful means.[60] The evidence need only be relevant and authenticated.

Some courts, however, have determined that they have the discretion to exclude evidence obtained in violation of ethical rules, despite the fact that ethical violations are principally handled through the attorney disciplinary system.[61] Having excluded evidence obtained through deceptive means, one court reasoned that "the desirability of deterring improper investigative conduct was a factor which the court could properly consider in the exercise of its discretion to exclude the evidence."[62]

In addition to potential exclusion of improperly acquired evidence, lawyers who participate in the improper collection of evidence may be punished for violation of ethical rules. Pretexting likely violates rules designed to ensure the truthfulness of statements to others.[63] In the course of representing a client, lawyers are prohibited from making false statements of material fact or law to a third person, and, generally, from engaging in dishonest conduct.[64] Moreover, lawyers are responsible for the violation of these rules by nonlawyers employed or retained by the lawyer to assist with an investigation.[65] Violation of these rules can result in public or private reprimand or, worse, disbarment. Violating laws or directing violation of laws can even lead to criminal charges and conviction.[66]

---

[60] *Stagg* at 780; *see also United States v. Parker*, 165 F. Supp. 2d 431, 477 (W.D.N.Y. 2001) (stating that even if attorney misconduct is deemed an ethical violation, "such does not warrant use of the exclusionary rule as a remedy for such violation.").
[61] Robert W. Sacoff, *The Ethics of Deception: Pretext Investigations in Trademark Cases* (April 1, 2010) at 5-10, available at http://www.pattishall.com/pdf/Ethics%20of%20Deception.pdf. (summarizing cases involving motions to exclude evidence); *see e.g. Midwest Motor Sports v. Artic Cat Sales, Inc.*, 347 F.3d 693 (8th Cir. 2003).
[62] *Trans-Cold Express, Inc. v. Arrow Motor Transit, Inc.*, 440 F.2d 1216, 1219 (7th Cir. 1971).
[63] Model Rules of Professional Conduct 4.1 and 8.4.
[64] *Id*.
[65] Model Rules of Professional Conduct 5.3.
[66] *See, e.g., United States v. Pellicano*, No. 2:2005-cr-1046, 2008 WL 859465 (Mar. 20, 2008 C.D. Cal.); *see also* Christopher Brett Jaeger & Gregory D. Smith, *Computer and Electronic Snooping Opportunities to Violate State and Federal Law*, 34 AM. J. TRIAL ADVOC. 473 at 473-75 (2011) (Terry Christensen, an attorney, was convicted for hiring Anthony Pellicano, a private investigator, to wiretap the ex-wife of MGM owner, Kirk Kerkorian. Pellicano may not have specifically told Christensen that he used an illegal wiretap, but it was determined that Christensen knew or should have known that Pellicano gathered the evidence in this way. That decision is currently on appeal. *United States v. Christensen*, No. 10-50472 (9th Cir., filed Sept. 29, 2010).

V. CONCLUSION

While social media evidence may have revolutionized the way humans interact, the law has been slow to catch up. By and large there are no special rules or procedures applicable to gathering social media before or during a lawsuit, nor are there special rules for using it at trial. The key is for in-house and outside counsel to remain conscious of outlets for social media evidence, and to ethically collect that evidence. Avoid pretexting and making any misrepresentations when gathering information. Diligence in collection is critical. You must acquire sufficient evidence to authenticate the evidence for trial and for summary judgment. Finally, do not ignore social media. It can be fertile ground for acquired evidence in litigation, as well as internal investigations.

10758972.3