III. Searching Social Media

Sara Anne Hook, M.B.A., J.D.

A. Common Social Media Sites and Where to Find Useful Information

Social media sites offer a wealth of possibilities for finding potentially relevant evidence. Of course, when most people think of social media, Facebook and LinkedIn may be the most popular. However, there are many other choices. For example, Bosack and colleagues note that "there is a vast universe about which in-house and outside counsel alike should develop a baseline knowledge. [Sean O'D. Bosack, Daniel J. Blinka, Laura A. Brenner and Kate E. Maternowski, *Social Media: Ethical and Practical Considerations for Collecting and Using Social Media Evidence in Litigation*. ABA Corporate Counsel CLE Seminar, Feb. 13-16, 2014, https://csdaca.org/wp-content/uploads/2015/04/W-47-Evidence-and-Social-Media-ABA-Litigation-Article-Handout1.pdf, accessed 9/12/17.] The authors divide social media into a variety of categories:

- Social Networks (Facebook, LinkedIn and Match.com)
- Media Sharing (YouTube, Instagram, Pinterest and Flickr)
- Activity Tracking (Nike + Running, FourSquare and GHIN.com)
- Blogs and Microblogs (WordPress and Twitter)
- Social News (Digg and Reddit)
- Discussion Forums
- Comments and Reviews (TripAdvsisor and Yelp) [*Id*. at 2-3.]

The authors indicate that

> 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. [*Id*. at 3.]

As these authors note, "social media data is fair game in formal discovery." [*Id*. at 8.] They go on to observe that "[p]rivacy objections have by and large proven unsuccessful

in preventing a party from obtaining another party's personal online data." [*Id*.] Fortunately, through the K&L Gates database of electronic discovery cases (https://www.ediscoverylaw.com/e-discovery-case-database/, accessed 9/12/17) and a similar service through Kroll Ontrack (http://www.ediscovery.com/pulse/case-law/, accessed 9/12/17), it is quite possible to find summaries of cases that deal with evidence from these various types of social media. Even though these cases may not discuss a particular service or vendor, they are helpful in illuminating some of the issues with requesting, obtaining and using social media as evidence.

For example, a quick search of the K&L Gates database (accessed 9/12/17) for cases on social media in 2017 found the following two summaries.

> *Brown v. Ferguson*, No. 4:15CV00831 ERW, 2017 WL 386544 (E.D. Mo. Jan. 27, 2017). Disclosure of passwords was not required and not permitted by the Federal Rules of Civil Procedure. Note that this case involves FRCP 26(b)(1) Scope in General (effective Dec. 1, 2015) – the amended version of this rule.
>
> *Gordon v. T.G.R. Logistics, Inc.*, No. 16-cv-00238-NDF, 2017 WL 1947537 (D. Wy. May 10, 2017). In this personal injury case, Defendant requested production of Plaintiff's entire "Facebook account history" for her two accounts (and later limited the relevant timeframe of the request to information from three years prior to the accident through the present). In response, Plaintiff produced information that referenced the at-issue auto accident or her injuries and also provided information identified by a set of keywords set forth by Defendant. She objected to further production based on a lack of relevance, undue burden, and invasion of privacy. The court granted Defendant's subsequent motion to compel, but imposed significant limits on the scope of production. Likewise, this case also applies that December 1, 2015 version of FRCP 26(b)(1) Scope in General (effective Dec. 1, 2015). Note that a longer summary of this case is available as well as a link to the judge's order on the Motion to Compel.

It is always useful to search both of these case databases. An interesting case from 2016 appeared when searching the Kroll Ontrack database (accessed 9/12/17) that deals with the court's willingness to compel a party to produce social media, particularly when the party does not disclose the existence of social media accounts.

Rhone v. Schneider Nat'l Carriers, Inc., 2016 U.S. Dist. LEXIS 53346 (E.D. Mo. Apr. 21, 2016) In this personal injury case, the defendants moved to compel the plaintiff to produce her "Download Your Info" report from Facebook, from the date of the accident to the present. The plaintiff objected that the request, arguing that it was overbroad as found in FRCP 26(b)(1), and moot because she already submitted hundreds of pages of Facebook postings. The court found that the plaintiff did not comply with the discovery request, since the "[p]laintiff did not initially disclose the existence of any social media accounts," and ordered the plaintiff to produce the requested information. In reaching its decision, the court noted the insufficiency of the plaintiff's objection, stating, "[a]lthough Plaintiff maintains that [defendant's] request is overbroad and asserts that such a production would be unduly burdensome, Plaintiff does not explain how it is overbroad or burdensome."

Other cases from the Kroll Ontrack database (accessed 9/12/17) are instructive about the delicate balance between social media requests that are specifically tailored versus overly broad. What the court typically wants to avoid is a "fishing expedition." On the other hand, the court is not going to be pleased if there is evidence that a party is either hiding the existence of social media accounts or has tampered with them so that potentially relevant evidence is no longer available.

Scott v. United States Postal Serv., 2016 U.S. Dist. LEXIS 178702 (M.D. La. Dec. 27, 2016) In this personal injury case, the defendants moved the court to compel discovery of certain of the plaintiff's social media accounts and postings, due to the plaintiffs' untimely discovery responses. The defendant had requested all postings related to any type of physical or athletic activities from the date of the accident that were present on all social media websites. The plaintiff rejected the defendant's requests as "inclement, immaterial and not reasonably calculated to lead to the discovery of admissible evidence." The court recognized that social media is discoverable under Fed.R.Civ.P. 34 and what defendants sought was relevant to the case, but that the defendant's requests were overly broad. The court stated, "[A] request for discovery must still be tailored so that it appears reasonably calculated to lead to the discovery of admissible evidence. Otherwise, the Defendant would be allowed to engage in the proverbial fishing expedition . . ." The court limited the defendant's requests to the plaintiff's social media postings from the date of the accident to present that related to the plaintiff's alleged physical injuries as a result of the accident, or physical capabilities that are inconsistent with the injuries that plaintiff allegedly suffered as a result of the accident. The court found that the language of the plaintiff's objections were too boilerplate, and that because the objections were not filed timely under Fed.R.Civ.P. 33(b)(2) and 34(b)(2)(A), were therefore waived.

Baxter v. Anderson, 2016 U.S. Dist. LEXIS 110687 (M.D. La. Aug. 18, 2016) In this personal injury case, the defendant moved the court to compel a wide range of discovery related to the plaintiff's social media accounts. The plaintiff objected to these requests as being "overbroad and unduly burdensome." The court noted that generally social media information is discoverable, but also noted the requests were indeed overly broad as written. Using the newly amended FRCP 26(b)(1), the court granted the motion to compel, but the court limited the information that was discoverable. The court restricted the scope of discovery to the date of accident and forward and also limited the production to only the documents that satisfied one of six criteria. The criteria indicated that the documents must be related to any references of the accident, or that contained references to physical injuries or emotional distress from the accident, or any "unrelated physical injuries suffered…by Plaintiff." The court cited precedent, which stated, "Simply placing their mental and physical conditions at issue is not sufficient to allow [Defendant] to rummage through [Plaintiffs'] social media sites."

Thurmond v. Bowman, 2016 WL 1295957 (W.D.N.Y. Mr. 31, 2016). In this Fair Housing Act case, the defendants motioned for sanctions against the plaintiff for deleting Facebook posts. The plaintiff argued that the posts were not deleted intentionally, but rather they were "hidden" from public view. The plaintiff produced a printed set of Facebook posts, which supplied most of the missing posts, but three posts remained missing. The court found that these posts, because of their nature (photographs of the plaintiff's children, supplied as "screen shots" by the defendants), were not relevant to the case. In addition, rather than relying on public privacy settings, the court noted that the defendants could have requested the information through discovery. The court denied the defendants' motion, stating that the claim that every social media post is relevant "sweeps far too broadly." However, because the plaintiff did change privacy settings in violation of a court order to maintain the "status quo" of social media accounts, the plaintiff was warned that further conduct in this manner could result in sanctions.

Other sources of information on electronic discovery, digital forensics and litigation support the websites for Sensei Enterprises, Inc. (https://senseient.com/, accessed 9/12/17) and Exterro, Inc. (https://www.exterro.com/, accessed 9/12/17; *See* The Simplified E-Discovery Case Law Library at https://www.exterro.com/case-law-library/, accessed 9/13/17.)

More recent forms of social media, such as Snapchat and WhatsApp, have some unique features and functionality that may make the collection of social media evidence

from these services. [*See* Cori Faklaris and Sara Anne Hook, *Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik and Other Mobile Messaging Apps*. The Federal Lawyer, 63 (4):64-75, May 2016.] Other possible social media sites that have been mentioned in requests as part of discovery are MySpace, Live Journal, Tagged, Meetup, myLife and MeetMe. (*Keller v. National Farmers Union Property & Casualty Co.*, 2013 WL 27731 (D. Mont. Jan. 2, 2013). New social media platforms and services are being introduced on a regular basis and others have disappeared. Thus, the lawyer needs to keep abreast of what is happening with communications technology and define requests to opposing parties and litigation hold orders for his/her own clients broadly enough to encompass all of these possibilities.

In an article on the impact of social media on litigation, Ettari and Syverson advise that:

> Social media is a fantastic tool for discovering potential evidence for an affirmative case or defense—like any other form of evidence, social media platforms should not be overlooked as a potential source of information. In the formal discovery process, it should be routine practice to include a request for the search and review of social media platforms in discovery requests if the underlying subject matter of the dispute provides a good-faith basis for belief that there is social media evidence relevant to the litigation. Many courts across the country are allowing discovery of social media, regardless of privacy settings. If you put something out there on a social media platform and it is responsive to discovery and relevant to the litigation, it will likely be ordered produced. Of course, there are ethical considerations when—outside of formal discovery—an attorney is doing informal discovery through online research of an adversary or witnesses, but that's slated for discussion below. [Nicholas Gaffney, Samantha V. Ettari and Erik S. Syverson, *Social Media's Impact on Litigation*. Law Practice Today, Nov. 13, 2015, http://www.lawpracticetoday.org/article/social-media-litigation/, accessed 9/12/17.]

The authors go on to observe that "[p]rivacy settings on social media accounts are not likely to keep relevant evidence from being discovered. Many courts have taken the position that if you posted a comment or a photograph to social media, despite the tightest privacy settings, the material is still discoverable." [*Id*. at 4.] The authors note that one of the issues with social media as evidence is authentication and the rules on this are still

developing. Another challenge that they identify is privacy settings, particularly in criminal law cases, and caution lawyers about invasion of privacy statutes as well as the Computer Fraud and Abuse Act or the Electronic Communications Privacy Act. [*Id*.]

In addition to rules related to civil procedure and evidence, there are can be ethical issues with social media that all lawyers and members of the legal team need to be aware of. McPeak provides an excellent article on some of the ethical issues with using social media investigation as part of litigation and the extent to which the ABA Model Rules of Professional Conduct provide sufficient guidance for lawyers. [Agnieszka McPeak, *Social Media Snooping and Its Ethical Bounds*. 46 Ariz. St. L.J. 845 (Fall 2014)]. In this substantive article, the author considers the duty to investigate facts, the no-contact rule and duty to avoid deception and the duty to advise client about social media and spoliation issues. Within the section on the no-contact rule and the duty to avoid deception, the author discusses social media's potential for violation of the no-contact rule and attempts to gain access to an unrepresented party's private content, including through fake profiles, direct requests by the lawyer and access through a third party.

Apart from specific issues with the discovery of social media as evidence, the lawyer is under an overarching duty to understand the ethical issues with using technology as part of the ABA Model Rules of Professional Conduct, as adopted in whole or in part, by the state or states where the lawyer is licensed to practice. As stated by Schweihs and Pesale, in the context of failing to provide data preservation advice that reflects current technologie***s***:

> While *Allied Concrete Co. v. Lester* provides a clear warning for attorneys regarding sanctions for intentional spoliation, lawyers can still be found liable for not demonstrating adequate technical competence when advising their clients.
>
> Twenty-six states have so far adopted amended ABA Model Rule 1.1, Comment 8's advisory duty for attorneys to keep abreast of the benefits and risks of relevant legal technology into their state ethics codes. Florida even mandates

> that attorneys take at least 3 CLE credits per reporting period in technology competency. Therefore, it would be advisable to consult your state's ethics rules to determine if you meet its minimum technological competency standards. [Patrick Schweihs and Eric Pesale, *Common Ethical Issues to Consider When Researching Jurors and Witnesses on Social Media*. Above the Law, Mar. 14, 2017, http://abovethelaw.com/2017/03/common-ethical-issues-to-consider-when-researching-jurors-and-witnesses-on-social-media/, accessed 9/12/17; *See also Thurmond v. Bowman*, 2016 WL 1295957 (W.D.N.Y. Mr. 31, 2016). Summary provided from Kroll Ontrack

Note that although a recommendation to add Comment 8 to the Indiana Rules of Professional Conduct was discussed as part of the Future of the Provision of Legal Services Committee of the Indiana State Bar Association, such language has not yet been incorporated.

Sweis comments on the wealth of information that is available on social media platforms. [Alexander Sweis, *Social Media: New Tool for Litigation Defense Attorneys*. McKenna Minutes, July 4, 2016, https://www.mckenna-law.com/blog/social-media-new-tool-litigation-defense-attorneys/, accessed 9/13/17.] He observes that:

> Google, Tumblr, Instagram, YouTube, Facebook and LinkedIn are only a few of the social media platforms on which plaintiffs and their friends post photographs, videos and written messages that can be freely accessed by anyone with access to the internet. The information that is available to defense attorneys can be used in personal injury cases and commercial litigation as evidence to prove or disprove key facts and allegations. What better way to challenge a plaintiff's claims of suffering a serious injury than with a series of photos showing the supposedly-injured party skiing with friends a short time after the accident. [*Id*. at 1.]

He goes on to advise that "[o]btaining a plaintiff's Facebook history can usually be accomplished during the discovery phase of a case with a request for production without having to resort to a subpoena." [*Id*. at 2.] As he reports, judges have been included to grant these requests when he has litigated a plaintiff's objection to providing the information from a social media account. [*Id*.]

B. Locating Hidden or Private Accounts

The lawyer who is representing the client should be very clear when asking about the social media sites that the client participates or has participated in and should caution the client that he/she is expected to preserve the information in profiles and accounts. The lawyer who fails to do this is not fulfilling his/her professional responsibilities and may even be subject to discipline under a state's rules of professional conduct. Moreover, expecting the court have to take the time and expense to continue to issue discovery orders for this material will not be prudent. Although we tend to think that only "young" people participate in social media, it is the rare person, indeed, who does not – or has not – at least had a basic account at some point.

A client's lawyer must be familiar with the December 2015 amendments to the Federal Rules of Civil Procedure, particularly Rule 37(e), which provides better guidance on what constitutes spoliation and when sanctions can be imposed, as well as Rule 37 as a whole. [Federal Rules of Civil Procedure, as amended to December 1, 2016, Rule 37, Failure to Make Disclosures or to Cooperate in Discovery; Sanctions. Legal Information Institute, https://www.law.cornell.edu/rules/frcp/rule_37, accessed 9/13/17.] Note the comments by Bosack and colleagues about the *Lester v. Allied Concrete Co.* case [(Nos. CL.08-150, CL09-223 (Va. Cir. Ct. Sept. 1, 2011); Lester v. Allied Concrete Co., Nos. CL08-150, CL09-223 (Va. Cir. Ct. Oct. 21, 2011) – "Where counsel instructed his client to "clean up" his Facebook page and his client therefore deleted a number of potentially damaging photographs and where counsel later submitted an inaccurate privilege log and then attempted to blame his paralegal, the court imposed monetary sanctions on both client and counsel." summary from K&L Gates, accessed 9/13/17.]

> As with all evidence, parties may not conceal or destroy social media evidence. In *Lester v. Allied Concrete Co*., the action 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.

> 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 account because "we don't want blowups of this stuff at trial." Defense counsel filed a motion to compel discover 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. [Bosack at 12.]

As stated by Fallon, "[u]nlike the ill-fated advice of the Virginia lawyer, establishing privacy settings does not destroy evidence, but simply makes such evidence more difficult for your adversaries to locate moving forward." [Fallon at 1-2.] A publication from i-Sight indicates that "[d]eleting photos, posts and other information is akin to shredding documents and courts have been clear about the consequences, handing out hefty fines and sanctions for spoliation…." [*How to Gather Social Media Evidence: Avoid Legal Disasters and Win Cases*. i-Sight, n.d., https://i-sight.com/wp-content/uploads/2012/02/How-to-Gather-Social-Media-Evidence.pdf?x96885, accessed 9/13/17.]

The opposing party's lawyer should be sure to consider requests for relevant evidence that encompass all types of social media, including those mentioned in Section A. of this chapter as well as any new providers, formats or types of data (including wearable health devices and the Internet of Things). Careful questioning should be used to ascertain the person's current and past accounts and participation. As Fallon recommends,

> Propound specially prepared interrogatories seeking the user name and password of sites with information known to be relevant to the issues in your lawsuit, which is similar to obtaining a HIPAA authorization to obtain medical records. Propound requests for production sufficiently particular to call for communications and photographs germane to the litigation, which fall within the definition of "writings" under Evidence Code Section 250. [*Id*. at 2.]

As he concludes, “[t]hese proposed methods of discovery may bear fruit or simply frustration, but in either scenario you will pressure your opponents and leverage your grasp of evolving technologies to the advantage of your client.” [*Id*.]

C. What to Do When You Can't Get Into an Account

Most commentators advocate that requests for information from social media profiles, particularly the private/non-public sections of a profile, should be made directly to the users of these accounts. The court has the opportunity to enforce these requests through its normal rules and processes. One recommendation that is clearly supported in case law is that discovery requests, particularly for social media, be carefully tailored. [Bosack at 11.] Another observation from Bosack and colleagues is that not all that appears to be deleted is lost. [*Id*. at 12.] As they note,

> 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. 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." [Id. citing Facebook's policies, updated at https://www.facebook.com/help/359046244166395/, accessed 9/13/17.]

Adee discusses what happens to social media profiles and the content within them, noting that "[t]he precise workings of deleting accounts or history with other companies is similarly unclear." [Sally Adee, *Is it Possible to Permanently Delete a Social Media Profile?*, New Scientist, July 27, 2015, https://www.newscientist.com/article/dn27958-is-it-possible-to-permanently-delete-a-social-media-profile/, accessed 9/13/17.] In addition to reviewing Facebook's policies, she reports that while Google lets you delete your search history, it does keep the search logs but disassociates them from your Google account so that they are anonymized. [*Id*. at 2.] However, the author reveals that data anonymization is becoming increasingly unrealistic, because re-identifying supposedly anonymized has been demonstrated many times and will only get easier as re-identification techniques become more sophisticated. [*Id*. at 2-3.] The lesson here is that even if a party claims to have deleted his/her profile, account or history, some of the data it is likely still available somewhere and can be pursued through the court and perhaps with the help of a digital forensics professional if

the argument can be made that such information is relevant to the case and that the burden of the extra time and expense necessary to retrieve and reconstruct it is worth the benefit.

Many lawyers may believe that the best way to obtain information from social media sites is to go directly to the providers. However, it is likely that these companies will refuse to do so, citing the Stored Communications Act (SCA) and a chain of cases starting with *Crispin v. Christian Audigier, Inc.* (717 F. Supp. 2d 965 (C.D. Cal. 2010.)). As noted by Bosack and colleagues, the SCA generally prohibits any entity that provides electronic communication service or remote computing services from disclosing the contents of a user's communications to non-government entities without the user's consent. [Bosack at 13.] As the authors explain, the SCA "shields from civil subpoenas providers and networks that send and store electronic communications for their users." [*Id*.] However, the authors note that the SCA does provide numerous exceptions for government access to user data without user consent. [*Id*.] As the authors observe,

> 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 suggests that 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. 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 discover… [*Id*.]

This advice is complemented by Fallon.

> As discussed in *O'Grady v. Sup. Ct.* (2006) 139 Cal.App.4th 1423, the Stored Communications Act (18 U.S.C. § 2702) renders unenforceable civil litigation subpoenas to internet service providers for information regarding their users. This means Facebook and other social media providers can refuse to comply with a civil subpoena requesting user data. Instead, parties must seek such information directly from their opponents, who are going to do everything in their power to avoid disclosure. [Fallon at 2.]

D. Friending/Following to Gather Evidence

Commentators have provided considerable insight into these tactics and most caution that "friending" or "following" could violate one or more of the ABA Rules of Professional Conduct. Bosack and colleagues refer to this conduct as "pretexting" and note that using a false identity to try to inveigle information from a party of witness likely violates one or more of the ABA Rules of Professional Conduct, including Rules 4.1, 8.4, 5.3 and 4.2. [Bosack at 4-5, 20.] These authors discuss the issues with evidence that is obtained illegally and whether it will be admissible. Fallon refers to this behavior as "predatory friending" and discusses it in the context of California's Rule of Professional Conduct 2-100(A) and the San Diego Bar Association's Legal Ethics Opinion 2011-2, observing that these prohibitions apply whether it is the lawyer, the paralegal, a claims representative or an investigator who is engaged in this activity. [Daniel P. Fallon, *Don't Delete that Photo! Social Media Investigations and Predatory Friending*. TMNews, Mar. 2014, http://www.tysonmendes.com/blog-predatory-friending/, accessed 9/13/17.] Ettari and Syverson, in answering the following question, provide some helpful information, including ethics opinions issued by states, municipalities and the highly-respected Sedona Conference:

> What are the ethical considerations when connecting with opponents on social media? May lawyers use false names or accounts to gather potentially damaging information?
>
> SE: If by opponent, you mean an opposing party, there are ethics rules governing this area of social media use as well, and it is a thorny area. Generally, a lawyer may not access private or non-public portions of a represented party or witness's social media accounts if in order to do so the lawyer would have to "friend" or "follow" the account holder. In New York, recent ethics guidelines and decisions have approved a lawyer friending an unrepresented individual without disclosing the reason for the request as long as it does not involve any type of trickery. Using a false name to mask the lawyers identity would fall within that prohibition. In fact, some ethics committees (such as in New Hampshire and San Diego) issued opinions requiring a lawyer to both use his real name and also identify the client, the matter, and his role in the dispute. The Sedona Conference also cautions against this kind of deceptive behavior as being a potential ethics violation.

ES: I don't see any ethical problem with that. I consider that work product and investigation. [Gaffney, Ettari and Syverson at 3-4.]

Note that any prohibitions extend to the lawyer's employees as well a third party vendors and contractors. For example, as reported in 2012, in New Jersey, the lawyers instructed their paralegal to "perform a broad and general internet search" for information relating to the plaintiff and never instructed her to actually friend the plaintiff. [Eric Meyer, *Ethics Charges for Two Lawyers Over Facebook Friending a Litigant*. LexisNexis Legal Newsroom: Labor and Employment Law, Sept. 13, 2012, https://www.lexisnexis.com/legalnewsroom/labor-employment/b/labor-employment-top-blogs/archive/2012/09/13/ethics-charges-for-two-lawyers-over-facebook-friending-a-litigant.aspx, accessed 9/12/17.] Further, both lawyers denied being familiar with Facebook's privacy settings. Note that the paralegal did use her real name when making the "friend" request. As reported, the attorneys involved were charged with violating multiple provisions of the rules of professional ethics, including those governing communications with represented parties, failure to supervise a non-lawyer assistant and conduct prejudicial to the administration of justice. [*Id*.] The article concludes that while New Jersey at the time did not have a published opinion on lawyers and their agents using Facebook to friend litigants, such opinions had been issued by bar associations in Philadelphia, New York City and San Diego. The author provides three lessons from the incident:

1. **Lawyers and HR professionals must have a basic grasp on social media.** As the report suggests, naiveté has its price.
2. **Lawyers should not friend represented parties.** At the very least, doing so would violate the rule of professional ethics that directly addresses this issue. Similarly, lawyers should not have an agent Facebook friend represented parties. However, IMHO, if a plaintiff, prior to taking legal action, is a Facebook friend of an employee of the defendant, I see nothing wrong with asking (but not requiring) that the employee obtain privacy-protected Facebook information from the plaintiff that is not publicly available in order to use that information to defend the lawsuit. Similarly, I see no reason why the plaintiff couldn't access private Facebook information that would benefit his/her case from one of the defendant's employees. I also think it makes sense

for plaintiff's counsel to Facebook friend the client to see what's there before I do.

3. **Lawyers: Do not let anything in this post dissuade you from researching litigants -- represented or not -- online.** Anything public is fair game. I have gotten the goods on many plaintiffs who, intentionally or not, failed to adjust their online privacy settings so that I, and the rest of the world, could see what they have posted. Heck, I would argue that you have an affirmative duty to conduct a diligent online investigation. Otherwise, you may miss ascertaining valuable online information relating to your case. Plaintiffs' bar, for heaven's sake, tell your clients to adjust their Facebook privacy settings. [*Id*.]

Schweihs and Pesale also discuss the distinction between research for information on social media that is publicly available versus attempting to access information that is private or encrypted. Note that their article is primarily focused on researching jury members or witnesses:

> Generally, lawyers can access public, published social media content without risking ethics violations. In fact, the American Bar Association (ABA) and some state court opinions have held that publicly-available social media data is discoverable in its own right, even if the social network itself notifies particular witnesses or jurors that specific attorneys are researching their profiles.
>
> Problems will arise, however, for lawyers looking to initiate contact with witnesses and jurors on social media or to obtain private or encrypted data through deceit. Under ABA Model Rule 3.5(b) and similar state ethics codes, an attorney cannot unilaterally initiate communication with a judge, juror, prospective juror or other official unless authorized to do so by a court.
>
> In the social media space, this covers messaging, tweeting at, and sending friend or connection requests to interested parties, whether by the attorney, a paralegal or other agent acting on behalf of the attorney. [Schweihs and Pesale at 2.]

As stated by Muse, among the many ethical rules that may be violated when a lawyer uses social media during case investigation and discovery, with the most common being Rule 1.6 Confidentiality of Information, Rule 4.1 Truthfulness in Statements to Others, Rule 5.3 Responsibility Regarding Nonlawyer Assistants (now Assistance) and Rule 8.4 Misconduct. [Seth I. Muse, *Ethics of Using Social Media During Case Investigation and Discovery*. ABA Section of Litigation: Pretrial Practice & Discovery, June 13, 2012,

http://apps.americanbar.org/litigation/committees/pretrial/email/spring2012/spring2012-0612-ethics-using-social-media-during-case-investigation-discovery.html, accessed 9/12/17.] The author then discusses the opinions of the New York State Bar Association, the New York City Bar Committee on Professional Ethics and the Philadelphia Bar Association Guidance Committee.

Additional guidance on using social media effectively as part of litigation while avoiding potential ethical breaches is provided by Sobel and Ettari. [Lauren N. Sobel and Samantha V. Ettari, *Social Media Tips and Ethics for Litigators*. Legal Solutions Blog, Mar. 15, 2017, http://blog.legalsolutions.thomsonreuters.com/legal-know-how-guidance/social-media-tips-and-ethics-for-litigators/, accessed 9/13/17.] Describing social media as a "treasure trove" of information that can be extremely useful if collected properly, the authors particularly discuss what can and cannot be done when searching social media from and ethical standpoint, including that social media must be preserved, what to advise the client about his/her privacy setting and the duty to preserve, the need for care when researching potential jury members and that social media is not a license for a "fishing expedition." [*Id*. at 1-2.] They go on to provide some specific information about the notion of "friending" or "following" as a way to gain access to non-public information from a social media profile.

> **2. Ethical rules apply to social media communication.** Although the content and proliferation of social media may suggest a free-for-all, ethical rules apply to attorneys using social media to gather information. Ethical rules may allow an attorney to use social media platforms to contact an unrepresented witness or party, but only if the attorney does not engage in deceptive behavior in the process. For example, an attorney cannot ethically create a fake Facebook profile with inaccurate information for the purpose of "friending" an unrepresented witness or party to gain access to their non-public posts, photographs, and the like. Many jurisdictions have published ethical guidance on these and other social media issues. Attorneys should become familiar with guidance in their jurisdiction before using social media for a case.
>
> **3. Know the difference between public and non-public information.** When investigating a case, publicly-accessible information on social media is typically fair game. Generally, however, an attorney may not attempt to access non-public

> information for use in litigation by "friending" a represented person or "following" their social media account, as that violates the prohibition against communicating with represented parties. [*Id*. at 1.]

Rotunda provides additional information about social media as it relates to witnesses, parties, jury members and clients, applying the ABA Model Rule of Professional Conduct and citing opinions from the New York State Bar Association's Committee on Professional Ethics, the Philadelphia Bar Association and the Committee on Professional Ethics of the Association of the Bar of the City of New York as well as the court in *Lester v. Allied Concrete Co*. [Ronald D. Rotunda, *Using Facebook as Discovery Device*. Verdict: Legal Analysis and Commentary from Justia, Aug. 4, 2014, https://verdict.justia.com/2014/08/04/using-facebook-discovery-device, accessed 9/13/17.] He concludes that:

> As evidenced by these examples, the ethical rules regarding the use of Facebook and other social media are in a state of flux and are rife with misunderstandings of how these sites work. It will be interesting to see whether they can catch up and adequately regulate lawyers' various uses of social media in the context of litigation. [*Id*. at 9-10.]

Likewise, Sweis notes that

> Attorneys must abide by ethical standards when attempting to gain access to posts and activities that the owner of the page has labelled as "private." State ethical guidelines may place restrictions on an attorney's ability to access private information. For example, the Illinois Rules of Professional Conduct prohibit attorneys from accessing social networking sites using false pretenses, such as "friending" the unsuspecting individual or having someone do so on the attorney's behalf. [Sweis at 1.]

He advises that because the rules that apply to accessing social media may be different in one jurisdiction versus another and because of the ethical opinions issued by state and local bar associations, lawyers should check with their bar associations for clarification of what is allowed. [*Id*.] An article from i-Sight confirms the risks with "friending" and notes that "[e]vidence gained by this kind of deception has not held up so far. It also violates the terms of service set out by some social media platforms and has prompted

some states to address the practice in writing." [i-Sight at 4.] This publication cites California Penal Code 528.5 and the Connecticut Rules of Evidence Section 52-184a.

E. Recovering Deleted Data

Recovering deleted data is a responsibility that often should be delegated to a digital forensics professional who has the skills and experience to do this properly using the standards and best practices of this important part of an electronic discovery process. Nelson and Simek advise that, regardless of the size of the digital forensics company you choose, some of the factors to consider in selecting the digital forensics expert are:

- Forensics certifications
- Technical certifications
- The expert's vita
- Beware of "the jack of all trades"
- Beware of "point and click"
- Court qualifications
- Confidentiality
- Geography may not matter
- English 101 and 201
- The price tag
- References, references, references [Sharon D. Nelson and John W. Simek, Finding Wyatt Earp: Your Digital Forensics Expert. Sensei Enterprises, Inc., May 21, 2016, https://senseient.com/articles/find-wyatt-earp-digital-forensics-expert/, accessed 9/13/17.]

As Hubbard notes,

> With nearly 1.8 billion users worldwide, Facebook has maintained its status as the platform of choice for users looking to share details of their personal lives publicly. If searched the right way, Facebook can be a treasure trove of discoverable data for litigators and litigation support professionals. Whether for initial research or for court evidence, if you're wondering how to collect social media data on Facebook, these four tips will help guide your social media investigation research in the right direction. [Kate Hubbard, *4 Ways to Conduct an Effective Social Media Investigation on Facebook*. Page Vault, Mar. 13, 2017, https://www.page-vault.com/facebook-investigation-tips/, accessed 9/13/17.]

The four steps that she recommends are:

1. Review a User's Profile Information for Discoverable Social Media Data. The author suggests that "[i]n addition to looking at Facebook's sections and features, you can also use your client's profile and those of consenting third-

parties in conjunction with other online tools to gather relevant evidence on profile visits for cyberbullying lawsuits and other civil and criminal cases." [*Id*. at 2.]

2. Conduct a Social Media Investigation of a User's Posts and Comments.

   As she notes, [l]itigators will likely find a user's published comments, notes and messages useful, not just for their content—which can, in part, touch upon a user's intent and state of mind or lead to discoverable evidence—but also for their embedded location data. If a user has Location Services enabled on Facebook, the content he/she publishes triggers geolocation data that can help pinpoint the Facebook user's location at the time they posted. For images specifically, Location Services can capture the EXIF data, which are metadata tags within an image that can include GPS coordinates. This information, which can oftentimes be found in the published content itself (i.e. John Smith at The Art Institute, July 15, 2016, Chicago, IL for a photo tagged by a friend), can prove useful in constructing case timelines or proving and refuting alibis. [*Id*.]

3. Conduct an In-Depth Social Media Investigation Using Advance Search.

   As she describes, Advance Search, the search engine within Facebook located at the top of the page, can be useful for conducting an in-depth social media investigation into a user's social profile. Obviously, the search feature wasn't created for legal web content collection, but rather for users searching for friends who have a similar interest in, for example, comic books. With that in mind, it works best if the user being researched is Facebook friends with your client or a cooperative third-party (check your local rules on the ethics of "friending" with others). [*Id*. at 2-3.]

   For legal professionals leveraging the tool, searches for phrases such as "Pages [User's Name] likes," for example, can return invaluable social media investigation results. Searches of phone numbers, email addresses, and other contact information can also help pinpoint owners of pseudonym or fake name profiles if they registered this information when signing up. [*Id*. at 3.]

4. Research User Data on Event and Group Memberships
   Collecting social media data on a user's event and group memberships can be useful for locating or finding leads for witnesses and interested parties for cases tied to particular events or local groups. Facebook also leaves public lists published for closed groups and past events, as well as active groups and upcoming events. [*Id*.]

> To find these results for a particular user, conduct searches within Search for phrases such as "Closed groups joined by [User's Name]" or "Events attended by [User's Name]." Test this tip out generally by typing in the Advanced Search bar "Closed Groups joined by my friends" and/or "Events attended by my friends" (you don't need to include the quotation marks). [*Id*.]

Note that Page Vault On Demand is marketed as a way for lawyers to submit requests for web content to be collected for initial research or as evidence and can help to capture discoverable data during a Facebook social media investigation. [*Id*.] As indicated, "[e]ach capture comes with key metadata (IP addresses, time/date stamps, URLs) that further supports the authentication of the content and that can be used as admissible evidence in court." [*Id*.] See www.page-vault.com/ondemand, accessed 9/13/17, for additional information.

The publication *How to Gather Social Media Evidence: Avoid Legal Disasters and Win More Cases* from i-Sight, *supra*, notes that there are relatively few standardized, widely accepted methods for gathering evidence from social media sites. [i-Sight at 5.] As indicated, a common approach is to print what is one the screen onto paper. [*Id*.] However, the authors note that printouts do not always contain all of the information and the interactivity that takes place on social media sites. [*Id*.] Therefore, a better alternative is a screencast. As described:

> A screencast captures the look, words, images, interactivity and interrelationships from one page to the next. It's a valuable tool because what's on a social media profile today may not be there tomorrow. Wright suggests using a webcast narration, where the investigator records a video of himself/herself talking about what they are seeing on the page. There are several effective tools for this, including Camtasia and Screencast-O-Matic.
>
> If what you're looking for is on Facebook, Meyer suggests using Facebook's "Download Your Information" function, which allows a user to create an electronic copy of his or her entire profile. This includes contact information, interests, groups, wall posts, photos and videos, friends list, notes, events, private messages, comments and other related content. [*Id*.]

The publication concludes with some recent case examples and court decisions.

Many digital forensics companies provide a variety of services for obtaining information from social media that has supposedly been "deleted" or that a party claims is no longer available. For example, Belkasoft's website indicates that it can recover and extract social network conversations and recover social network remnants via Live RAM analysis. [*Recover Social Network Conversations,* Belkasoft, n.d., https://belkasoft.com/recover-social-network-conversations, accessed 9/13/17.] According to the website, the data may include conversation threads and individual chat messages (for most social networks, including Facebook and Twitter), email messages sent with Internet Explorer, Google Chrome and Firefox, sender and recipient information such as nicknames and account numbers, and date and time, subject and message body, sender's photo link, a link to a profile and the time the profile was last updated. [*Id*.]

Other companies may offer services to assist with recovering and analyzing information from social media sites. For example,

- Secure Data Recovery: https://www.securedatarecovery.com/services/forensics/social-media-analysis, accessed 9/13/17.

See also Keil Hubert, *Evidence Collection from Social Media Sites*. SANS Institute, Dec. 1, 2014, https://www.sans.org/reading-room/whitepapers/legal/evidence-collection-social-media-sites-35647, accessed 9/13/17.