To Post or Not to Post:
How Social Media Impacts Jury Selection and Discovery

Social Media in the Courtroom: Jury Selection and Discovery

It was only a matter of time before social media, as ubiquitous as it is in modern life, found its way into the courtroom. There are myriad ways in which this new form of communication and interconnection works its way into litigation and court proceedings, and not all of them provide benefits to litigators or judges. Two major areas in which social media has upended the traditional trial process are the jury selection and discovery process, and both present a cluster of complex issues that courts and policymakers are only now just starting to unravel.

I. Social Media and Jury Selection

Of all the ways that litigators are tempted to use social media at trial, perhaps the most straightforward and potentially risky is the use of social media during the jury selection process. Imagine a scenario where counsel is deadlocked on which jurors to strike after the voir dire process, when suddenly an idea emerges – why not check the Facebook pages, Twitter feeds or LinkedIn profiles of the potential jurors? Such a search on social media might be a quick and easy way to glean more information about the jurors that might not otherwise appear in the course of the voir dire process. The question then arises: is this social media search permissible or even ethical? Is merely reading a publicly-available Facebook page acceptable? What about sending a Facebook friend request or using a shared connection to link up on LinkedIn?

For several years, attorneys struggled with these questions about how much they could invade a potential juror's personal digital realm. Fortunately, the Standing Committee on Ethics and Professional Responsibility of the American Bar Association ("the Committee") provided much-needed guidance in April of 2014 in the form of Formal Opinion 466, "Lawyer Reviewing Jurors' Internet Presence." The general tenor of the Formal Opinion is that an attorney may view the public postings of jurors and potential jurors so long as the attorney comports with the provisions of ABA Model Rule of Professional Conduct 3.5, "Impartiality & Decorum of the Tribunal":

> "A lawyer shall not:
>
> > (a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law;
> >
> > (b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order;
> >
> > (c) communicate with a juror or prospective juror after discharge of the jury if:
> >
> > > (1) the communication is prohibited by law or court order;

> (2) the juror has made known to the lawyer a desire not to communicate; or
>
> (3) the communication involves misrepresentation, coercion, duress or harassment; or
>
> (d) engage in conduct intended to disrupt a tribunal."[1]

This rule firmly abolishes communications with jurors (or prospective jurors – the Formal Opinion considers both equally and with no distinction) before or during trial, which sounds like merely viewing a Facebook post may pass muster. As with any area of the law, however, there are more complex issues which must be parsed.

a. Websites v. Social Media

The Formal Opinion makes a dual distinction, separating "websites," defined as "publicly-accessible Internet media" from "electronic social media" ("ESM"), defined as "internet-based social media sites that readily allow account-owner restriction on access."[2] The Formal Opinion uses Facebook, MySpace, LinkedIn and Twitter as examples of commonly used ESM as distinct from standard websites. Some ESM sites may hold publicly-available information, making them similar to a website, but there is also the ability to restrict information to only those who have been given access. This distinction is important, and drives the rationale behind the opinion.

b. Three Scenarios for Social Media Review

The Formal Opinion uses the distinction between websites and ESM as the basis for three general scenarios an attorney may face with juror social media. The first scenario envisions an attorney looking passively at a juror's website or ESM that is available to the public without making some sort of request and where the juror is unaware that the website or ESM information is being seen by the attorney. The next situation involves more activity in that the lawyer requests access to the juror's ESM through a friend request or similar account connection. The final scenario is similar to the first in that the attorney is only passively reviewing the juror's website or ESM, but the juror becomes aware of the identity of the attorney through a feature of the site.

In the first scenario, if the attorney merely reviews the publicly-available information on a juror's website or ESM, the Formal Opinion finds no ethical violation. The opinion uses the analogy of a "drive-by" to bring the scenario out of the digital world and into the practical one: "In the world outside of the Internet, a lawyer or another, acting on the lawyer's behalf, would not be engaging in an improper ex parte contact with a prospective juror by driving down the street where the prospective juror lives to observe the environs in order to glean publicly available information that could inform the lawyer's jury selection decisions."[3] In other words,

---

[1] Model Rules of Prof'l Conduct R. 3.5 (1983).
[2] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466 (2014) at 1.
[3] *Id.* at 4.

looking at what the public can see does not constitute ex parte contact for purposes of Model Rule 3.5.

Unsurprisingly, the Formal Opinion does take the position that sending some sort of access request to a juror electronically as in the second scenario does constitute a form of ex parte contact. ESM allows a juror to cordon off information that is not available to the public. For example, Facebook allows privacy levels that restrict access to status updates, pictures and nearly any other piece of information on a user's profile. To attain access to that information, an attorney would have to send that user a "friend request." This sort of request implicitly asks for the juror to provide more information to the attorney, and this request crosses an ethical boundary under Model Rule 3.5. The Committee extended the drive-by analogy of the first scenario to apply to this second situation as well, likening a digital access request to "driving down the juror's street, stopping the car, getting out, and asking the juror for permission to look inside the juror's house because the lawyer cannot see enough when just driving past."[4]

Interestingly, the Committee does not address a further issue of whether it is permissible to view a juror's restricted ESM through the account of a third party that already has access. The opinion prohibits an attorney personally, or through another, from sending an access request to a juror, but it does not specifically prohibit the attorney from viewing the juror's account from the account of one with prior access. While this scenario may seem far-fetched, many people within a community may only have one to two degrees of separation from others. Networking features of sites such as LinkedIn show the degree of difference between one profile and another, linking the two along lines of mutual connection. It is possible that an attorney may have one or more mutual connections with a juror through social media sites and the ability to access restricted ESM without the juror knowing. Speculatively, it is worth noting that the analogy used by the Committee in the Formal Opinion may shed some light on this scenario, as it is unlikely that it would be ethical for an attorney to enter the house of a juror through the help of a mutual friend who possess a spare key. Still, the opinion makes much of the distinction between passive and active activity of the attorney vis-à-vis the juror, and such a passive viewing of information through a mutual contact would still not be direct contact with the juror, even by a mechanized means such as an access request.

It is the third scenario as outlined in the Formal Opinion that provides the most troubling ethical problem. An attorney may passively review a juror's LinkedIn profile, but LinkedIn contains a feature that notifies the user that his or her profile has been viewed as well as the identity of the viewer. The juror becomes fully aware that the attorney has viewed his or her profile. As of now, LinkedIn is the only form of ESM that has this feature, but other sites may evolve to include similar mechanisms.

The Committee struggled with this third situation, ultimately deciding in the Formal Opinion that such a review of a juror's publicly-available information is still a passive act and not a form of ex parte communication with the juror. The notice sent to the juror that the attorney viewed his or her profile is a mechanical action of the site in the eyes of the Committee, not a communication from the attorney in some form. In the view of the Committee, this form of communication is akin to a neighbor telling the juror that the attorney drove past his or her house. The Formal

[4] *Id.*

Opinion cited opposing views, however, from the Association of the Bar of the City of New York Committee on Professional Ethics and the New York County Lawyers' Association Committee on Professional Ethics, both of which found that the awareness of the review on the part of the juror might change the juror's perception or influence the juror's conduct.

c. Be Careful What You Look For – You Just Might Find It

Finally, the Formal Opinion addressed the potential consequences of an attorney's review of juror social media in that an attorney may discover more than he or she bargained for in such a review when a juror commits misconduct and uses ESM to discuss the pending case or jury service. In this instance, the Committee stopped short of creating a bright line rule to guide attorneys, instead standing behind a provision of Model Rule 3.3:

> "(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures including, if necessary, disclosure to the tribunal."[5]

The Formal Opinion cited the comment to this rule that touches on the lawyer's obligation to help protect the integrity of the adjudicative process, noting that the rule was expanded in 2002 to include an attorney's discovery of misconduct by any person, rather than merely the client of the attorney. The operative words in the rule are "criminal or fraudulent," however, which is where the Formal Opinion's analysis and answer leave much to be desired.

For instance, what is the lawyer's obligation when a juror engages in some form of misconduct that is not necessarily criminal or fraudulent? The Formal Opinion notes that the answer is unclear, at least where the Model Rules are concerned. An attempt by the Ethics 2000 Commission to place an affirmative duty on an attorney to report any instance of juror misconduct did not reach fruition, so the lawyer's obligation under Rule 3.3(b) is limited to instances of criminal or fraudulent conduct. The Formal Opinion only provides that in the instance where a juror's postings about a case during trial violate court instructions, the lawyer must decide him- or herself whether those postings rise to the level of contempt or violations of other criminal statutes as would trigger an affirmative duty to act. In other words, according to the Formal Opinion, lawyers are on their own.

With potential ethics violations or the potential to trigger an affirmative duty on the part of the attorney to report juror misconduct, some attorneys may take the warnings of the Formal Opinion as a sign that juror social media should best be left alone. The Formal Opinion does encourage lawyers to discuss with judges the court's expectations regarding attorney review of juror ESM, going so far to suggest that judges can limit such review if necessary or inform the jury about the potential for such review. If anything, lawyers would be best served by creating a consistent internal policy about reviewing a juror's ESM and consulting the judge at trial about the policy whenever possible. The Formal Opinion provides attorneys some leeway in viewing juror ESM, and in an adversarial system where even the smallest details could make or break a case, litigators should be quick to take advantage of the potential edge gained from using this modern, public source of juror information.

---

[5] Model Rules of Prof'l Conduct R. 3.3(b) (2002).

II. Social Media and Discovery

Social media provides a treasure trove of information for litigators. The types of data posted on a social media account provide a wealth of information about a user's state of mind, communications with others, physical location at a specific time, video or photographs of specific events, and more, all of which can be exceedingly useful at trial. The question then becomes how to request and process this data through discovery.

As noted with jury selection and social media earlier, ESM accounts restrict access and allow the user to control privacy settings to limit public view. Because of this, there are generally only three avenues to obtain social media information: asking the user directly for the information, viewing the user's information through a third party with access to the user's information, or pursuing the information through the social media portal itself.

i. Don't Subpoena Facebook

One of the first things that litigators should understand is that the Stored Communications Act ("SCA")[6] will stand as a potential bar to the subpoena of personal information from most sites directly. Facebook, for instance, states on its help page, "Federal law does not allow private parties to obtain accounts contents (ex: messages, Timeline posts, photos) using subpoenas."[7] Facebook will agree to provide only basic subscriber information and not content when served with a federal, California, or California domesticated subpoena, making such an attempt hardly worth the effort.

Courts have struggled with the question of whether social media content can be attained via subpoena of the site itself in light of the SCA. One of the first major cases to address the issue, *Crispin v. Christian Audiger, Inc.*,[8] held that social media service providers fall within the definition of electronic communication service ("ECS") under the SCA, and content requested by subpoena – to the extent it was private or restricted – was off-limits. Another case, *Romano v. Steelcase, Inc.*,[9] held that information sought by litigants was "material and necessary"[10] to the defense, but stopped short of holding that the SCA did not apply to social media. Instead, the court in that case ordered the plaintiff to execute a consent to access her social media records from Facebook and MySpace to effectuate the subpoenas with those sites. The court in *Romano* took an end-run around the SCA, as the permission of the user would override the SCA objections of social media sites and allow production of the requested content. The line of cases so far has largely interpreted the SCA to apply to social media, however, so a subpoena of content directly from a social media operator is not likely to result in success without the permission of the account holder.

---

[6] 18 U.S.C. § 2701 et seq.

[7] *Law Enforcement & Third-Party Matters*, FACEBOOK, http://www.facebook.com/help/473784375984502 (last visited July 17, 2015).

[8] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[9] *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (Sup. Ct. 2010).

[10] *Id.* at 430.

ii. Don't Ask for Too Much

While a direct subpoena to a social media site may be unlikely to bear fruit, production of social media information can be obtained from the users themselves. Indeed, many sites anticipate this particular use and provide means through which to accomplish it. Facebook, the world's largest social networking site by number of users (1.44 billion monthly active users)[11] and the second most popular site on the web by traffic,[12] provides a tool so that parties in discovery may download their Facebook information to comply with party and non-party discovery requests. Other social media sites may have similar functions. When submitting a discovery request for social media, however, counsel should avoid being too greedy. While there is a temptation to ask for everything and everything, there is also the requirement that the requesting party identify that the social media is discoverable and any evidence produced from such a request is likely to be relevant.

The key to successful discovery requests with social media is specificity. As with almost any discovery request, the court is liable to look with disfavor on a fishing expedition disguised as a request for production. Social media is no different, and courts will likely limit expansive requests before compelling production. Federal Rule of Civil Producer 34(b) states that a discovery request for electronically stored information ("ESI") "must describe with reasonable particularity each item or category of items to be inspected."[13] Users spend years online and post statuses, photos and comments on a daily basis, so compliance with Rule 34(b) will require honing in on relevant information. Besides, a request of the entirety of a user's account information would likely run afoul of Federal Rule of Civil Procedure 26(b)(2)(B), which places limits on discovery of electronically stored information when the sources are not reasonably accessible because of cost or another undue burden. Of course, Rule 26(b)(2)(C) provides the ultimate limitation on overly burdensome or expensive discovery requests when the burden or expense is likely to exceed the benefit of the evidence.

Additionally, revisions to Rule 26 set to take effect on December 1, 2015 clearly envision a fresh take on discovery of ESI. Proposed Rule 26(b)(1) deletes the phrase "reasonably calculated to lead to the discovery of admissible evidence," which could broaden discovery in a digital context significantly.[14] The Rule now also will provide that discovery must be both relevant and "proportional to the needs of the case,"[15] providing a further limit on electronic discovery that can quickly grow out of hand.

---

[11] *Facebook Reports First Quarter 2015 Results*, FACEBOOK, http://investor.fb.com/releasedetail.cfm?ReleaseID =908022 (last visited July 17, 2015).

[12] *The top 500 sites on the web*, ALEXA INTERNET, INC., www.alexa.com/topsites (last updated July 15, 2015).

[13] Fed. R. Civ. P. 34(b)(1)(A).

[14] *Advisory Comm. on Civil Rules*, U.S. COURTS (Apr. 1, 2014) at 98, available at http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-civil-procedure-april-2014 (last visited July 17, 2015).

[15] *Id.*. at 97.

iii. Who Gets to Review?

Although social media is discoverable, courts still also struggle with how much access to grant the requesting party. Again, courts are loath to allow fishing expeditions into a user's private social media accounts, so in addition to specificity, the next area of contention in the discovery process is in how the production will occur and to whom. Generally, there are three ways that courts will order discovery of social media – review by the party requesting the information, review by the producing party as delineated in a methodology determined by the court, and *in camera* review by the judge.

In the first, the court orders the producing party to turn over all user names and passwords to relevant social media accounts, or as mentioned earlier regarding the *Romano* case, consent for the social media company to turn over the information directly. The disadvantage of this form of production/review is that it allows the requesting party full access to all of the opposing party's account, including highly personal and irrelevant material. It also gives the requesting party a chance to fish. This form of review is used fairly often, but is seen by some courts as overly broad.

The second form of review is likely the most restrictive – the court fashions a sort of restrictive net that limits the amount of information available to the requesting party, or provides a set of guidelines that the producing party must follow to fulfill the request of the opposing party. In *EEOC v. Simply Storage Management, LLC*,[16] for instance, the court rejected the defendants' request for full access to the social media sites of the plaintiffs but also rejected a request by the plaintiffs for limitation to only certain communications that directly addressed the specific matters alleged in the complaint. The court instead set up a scope of discovery for the social media sites for a specific time period and with limitations (for instance, photos posted by the claimants in the case during the specific period were discoverable, but photos where claimants were merely "tagged" by a third party were not).

Finally, courts will take upon themselves the burden of searching social media for relevant content through *in camera* review. This is done as a means of protecting the privacy of the party required to produce the information, but to ensure also that all relevant data is provided to the requesting party. One cannot imagine that this is a particularly welcome outcome for a judge, but some have gotten creative with this concept. In the case of *Barnes v. CUS Nashville, LLC*,[17] the magistrate judge offered to create a Facebook account solely for the purpose of becoming a Facebook "friend" of two parties that took pictures of the Plaintiff in a slip-and-fall case. The judge was willing to review the profiles *in camera* for the purposes of determining relevance, deleting the judicially-created Facebook profile once the review was concluded.

iv. Authentication Issues

Of course, once the social media content is obtained, there is still no presumption of authentication. As with other exhibits, social media must be authenticated when used at trial. Federal Rule of Evidence 901(a) states "the proponent must produce evidence sufficient to

[16] *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430 (S.D. Ind. 2010).
[17] *Barnes v. CUS Nashville, LLC*, No. 3:09-cv-00764, 2010 WL 2265668 (M.D. Tenn. June 3, 2010).

support a finding that the item is what the proponent claims it is."[18] Rule 901(b) provides a series of examples for authentication. Magistrate Judge Paul W. Grimm, in the case of *Lorraine v. Markel American Insurance Company,*[19] used the examples in subpart (b) as a roadmap for the authentication of digital evidence.

The first step in the authentication process, set out in Rule 901(b), is the have the digital content authenticated directly by a witness with knowledge, such as the account owner. That step may be easy enough with a cooperative witness, but slightly more difficult when the user claims that he or she did not author the content issue or that his or her account was hacked.

The next step in the authentication process comes from Rule 901(b)(3), which allows expert witnesses or the factfinder to compare the proffered evidence to a specimen that has already been authenticated.

Rule 901(b)(4), Judge Grimm noted, is the one most frequently used to authenticate electronic records such as email, and it permits authentication by "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."[20] This form of authentication can be seen as a reliance on circumstantial evidence, but it also can include authentication by using "hash values" or "hash marks," unique numerical identifiers that can be inserted into documents, helping counsel to authenticate a party's own electronic records. Rule 901(b)(4) also allows authentication by examination of metadata, which is data stored within a file that is not related to the content of the file, such as the filename, file size, location, etc.

Rule 901(b)(7) allows for authentication via public records or reports if those records if those records can be shown to come from the legal custodian of the records.

Finally, Rule 901(b)(9) authorizes authentication through "[e]vidence describing a process or system and showing that it produces an accurate result."[21] This rule is particularly applicable to digital evidence, and as Judge Grimm discussed in *Lorraine*, the advisory committee note to the rule expresses that the Rule was specifically designed to cover computer-generated evidence.

v. Spoliation

The problem of spoliation is especially tricky in light of the fleeting and potentially temporary nature of social media. The rule is that all parties have a duty to preserve evidence when litigation is pending or reasonably anticipated,[22] and that applies equally to social media. From the outset, counsel in cases where social media could potentially become evidence should immediately take precautions to preserve such evidence, such as through the Facebook mechanism described earlier.

---

[18] Fed. R. Evid. 901(a).
[19] *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).
[20] Fed. R. Evid. 901(b)(4).
[21] Fed. R. Evid. 901(b)(9).
[22] Fed. R. Civ. P. 37(f) cmt. (2006).

It may be instructive, however, to learn from the mistakes of others. For instance, in *Allied Concrete Co. v. Lester,*[23] the plaintiff in a wrongful death suit over the death of his wife sent a message to the opposing party's counsel through Facebook. As a result, opposing counsel was able to view the plaintiff's Facebook page, upon which was a picture of the plaintiff holding a beer and wearing a shirt with the phrase "I ♥ hot moms" written across the front. Opposing counsel immediately issued a discovery request for the majority of the plaintiff's Facebook page, presumably because such material would be injurious to the plaintiff's status as a grieving husband at trial. Plaintiff's counsel immediately instructed him to "clean up" the Facebook page, and the plaintiff responded that he had deleted the page. The plaintiff then stated in an answer to the discovery request that he had no Facebook account, even though he had only deactivated and later reactivated the account. He also deleted 16 pictures from the account. This behavior resulted in sanctions against the plaintiff personally in the amount of $180,000, and as against the plaintiff's attorney in the amount of $542,000.

Courts have shown a willingness to impose Federal Rule of Civil Procedure 37 sanctions in instances where parties attempt to delete or deactivate accounts to avoid discovery or delete relevant evidence, so trial counsel should immediately take precautions to preserve any potential social media evidence as a way to protect against misconduct on the part of clients.

III. Conclusion

Social media can be a powerful and effective tool in the realm of jury selection and discovery, but as one can see, it can also come with serious pitfalls for the unwary. Social media's place at trial still finds itself in relatively uncharted waters, but the developing rules show that the key delineating feature of social media in any context is the distinction between truly public information and private, access-restricted content. The former is fair game, while the latter comes through the negotiation of significant hurdles, if at all.

- By: Robert T. Watson

Mr. Watson is the Member in charge of the Louisville, Kentucky office of McBrayer, McGinnis, Leslie & Kirkland, PLLC www.mmlk.com. He practices generally in the areas of commercial, constitutional and insurance litigation. He received his B.A. from Transylvania University and then went on to receive his J.D. from the University of Kentucky. Mr. Watson is a member of the Kentucky and Louisville, Kentucky Bar Associations and of the Defense Research Institute.

[23] *Allied Concrete Co. v. Lester,* 736 S.E.2d 699 (Va. 2013).