LITIGATORS' TOOLBOX: SOCIAL MEDIA

Sharon Nelson, John Simek, and Jason Foltin

INTRODUCTION

Social media has revolutionized our world. Six years ago, Facebook boasted a whooping one million users. Today, that number has reached well over 500 million. Just five years ago, there were less than 10 million YouTube videos watched per day worldwide. Today, that number has reached two billion. Similarly, five years ago most people had not heard of Twitter. Today, people post over 65 million tweets every day.

This change in how we communicate has increasingly transformed the way lawyers search for and conduct discovery in preparation for trial. Unfortunately, the law governing discovery of online personal information not precisely clear cut. Only a few courts have thus far directly addressed the issue. However, there are some guiding principles attorneys should follow when faced with social media discovery.

EVIDENCE OVERLOAD

Gleaning potentially relevant evidence from the mountains of information posted on social media sites might appear to be an insurmountable task to the uninitiated and, undoubtedly, many attorneys shy away from such discovery for that very reason. Many cases have demonstrated that doing so would be unwise; a single photo or e-mail can often determine the outcome of litigation. In 2010 alone, there were over sixty reported cases mentioning evidence obtained from social networking sites Facebook and MySpace. For instance, plaintiffs have unwittingly posted photos showing their physical prowess despite claiming permanent disabilities and individuals have publically threatened others via Facebook or Twitter. While, in

a majority of the cases, the evidence was not the smoking gun, the information could be used for impeachment purposes or simply to provide important background information on the clients.

OBTAINING EVIDENCE FROM THE PARTIES

So, how do you find or obtain information on social media sites? Ethically, first and foremost! Attorneys must always consider the ethical implications of obtaining information from social media sites by deceptive means. Often, this involves an attorney sending, or getting a third-party to send, a friend request to an adverse witness's private social networking page in order to discover impeachment evidence. Recent ethics opinions from the New York State, New York City, and Philadelphia Bar Associations ethics committees have addressed this particular issue and all three determined that any form deception or trickery to gain access to social networking pages was objectionable. Interestingly, New York City Bar Opinion 2010-2 (2010) noted that a lawyer could, so long as he identifies himself using his real name and profile, request friend status. It appears, however, that none of the three opinions have a problem with publicly available information; the New York State Bar Association Opinion 843 (2010) concluded that a lawyer may ethically view and access the Facebook and MySpace pages of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither friends nor directs someone else to do so.

That aside, there is some information that can be ethically obtained without formal discovery. As stated in the New York State Bar Association Opinion 843, any profile or post from a party, witness, or judicial that is public information is fair game. In fact, the court in *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125 (Ct.App. 2009), found that a post on an unrestricted MySpace page was open to the pubic eye and thus, the plaintiff had no reasonable expectation of privacy as to the content. That means that an attorney should always check and

see whether any individuals related to the pending litigation have a public profile on any social networking sites. If so, the attorney should periodically take screen shots of potentially relevant information if it becomes available.

If an individual has heightened security settings that will not allow general viewing of relevant information, the security setting must be respected. Remember, attempting to bypass these settings through deceptive conduct or trickery will likely run afoul of ethical rules and subject the attorney to disciplinary action or sanctions. This leaves the usual discovery process. Generally speaking, the basic discovery rules apply. Preservation issues will need to be discussed as soon as the lawsuit commences and again in the Rule 26(f) meeting of the Federal Rules of Civil Procedure. This step is particularly important given the fact that social media companies have the right to delete content they find objectionable even if pending litigation demands the preservation of that particular information. Certainly, a lawyer could take screen-shots to capture images of content located on the site, but those images are static and, as we are all well aware, content is added and changed constantly, so getting authoritative data that can be time-authenticated in court is an issue. Once preservation is addressed, lawyers should draft and send interrogatories to determine what sites, if any, a party uses, what the ISP addresses are, and what the passwords are. Then come Requests for Production, which should be broadly construed to capture any information – including photographs, wall posts, video, etc. – of any issue related to the lawsuit. Here, recent amendments to the Federal of Civil Procedure have addressed a party's requests for electronically stored information (ESI) and should cover any ESI requests from social networking sites. Rule 34 provides that "any party may serve on any other party a request (1) to produce…any electronically stored information – including…data or data complications stored in any medium from which information can be obtained…" Obviously,

these requests will likely be met with some resistance, as most of the information is either very personal or irrelevant. A recent line of cases has provided some insight into what is discoverable, albeit, the distinction between discoverable social media evidence and non-discoverable social media evidence is still hazy at best.

For example, in a recent New York case, *Romano v. Steelcase, Inc.*,[1] Defendant sought to discover Plaintiff's current and historical Facebook and MySpace pages and accounts, including deleted information, in the belief that information posted there was inconsistent with her injury claims. Plaintiff objected to Defendant's request, arguing, among other things, that her expectation of privacy trumped Defendant's need for access to said evidence. After first establishing that the information sought was clearly relevant to Plaintiff's personal injury claim, the court found that production of her MySpace and Facebook entries would not violate her right to privacy, and that any such concerns were outweighed by Defendant's need for the information. Specifically, the court noted that both Facebook and MySpace informed users that they were not guaranteed complete privacy; MySpace went so far as to warn users that their profiles and MySpace forums are *public* spaces. Concluding, the court stated:

> [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 setting. Indeed that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.[2]

As such, the court ordered Plaintiff to allow Defendant access to the requested information.

---

[1] 2010 WL 3703242 (N.Y. Sup. Ct., Sept. 21, 2010)
[2] *Id*. at 6.

Similarly, in *EEOC v. Simply Storage Mgmt., LLC*,[3] the court again considered a defendant's request for production of all social media content on two claimants' online profiles. Like the Plaintiff in *Romano*, the underlying objection to such production was that it would improperly infringe upon claimants' privacy and cause embarrassment. Defendant responded to this contention by noting that the information was proper because Plaintiff, *EEOC*, had placed the emotional health of the claimants at issue beyond the typical "garden variety emotional distress claims"[4] and that "the nature of the injuries…alleged implicates all of [claimants'] social communications (i.e., all their Facebook and MySpace content)."[5] Here, the court stated that while the "discovery of SNS requires the application of basic discovery principles in a novel context," the true nature of the challenge before it was to "define appropriately broad limits – but limits nevertheless – on the discoverability of social communications…and to do so in a way that provides meaningful direction to the parties."[6] Turning to the privacy concerns proffered by the Plaintiff, the court determined that the claimants' expectation and intent that their SNS communications would be maintained as private was not a legitimate basis for prohibiting discovery; that SNS content must be produced when relevant to the claim or defense in a case; and that the proper scope of discovery was wider than communications that directly reference the matters alleged. As such, the court determined that the proper scope in the instant case was:

> [A]ny profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and SNS applications for claimants…that reveal, refer, or relate to any emotion, feeling or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce significant emotion, feeling or mental state.[7]

---

[3] No. 1:09-cv-1223-WTL-DML (S.D. Ind. May 11, 2010)
[4] *Id*. at 3.
[5] *Id*. at 5.
[6] *Id.*
[7] *Id*. at 9-10.

In addition, the court also ordered the production of any third-party communications to claimants if they placed the claimants' own communications in context. Finally, the court required the production of photographs of the claimants because the context of a picture and the claimants' appearance might provide insight into the claimants' emotional or mental status. Wrapping up its discussion, the court once again turned to the issue of privacy. The court acknowledged the possibility of embarrassment but reasoned that this is the inevitable result of alleging these sorts of injuries and explained that this concern was outweighed by the fact that the production here would be of information claimants had already shared.

In the end, expect some give-and-take to occur over these discovery requests. More specifically, courts will likely balance the requesting party's need for the information with the opposing party's general expectation of privacy. Protective Orders are designed to handle such situations and can help shield personal and potentially sensitive information not relevant to the suit. It is also important to point out that the same general parameters will likely apply to third-party subpoenas requesting production of social media information related to a lawsuit; albeit, with one caveat: Courts will likely err on the side of protecting the privacy interests of third party rather than disclosure.

OBTAINING EVIDENCE FROM SOCIAL MEDIA SITES

So far we've been talking about requests to individuals, but what about subpoenas to a social networking site? If the site gives the okay and the opposing party does not object, then discovery is very straightforward and usually explained on the social media site. Unfortunately, this is not usually the case; your request will probably be met with an objection by the site or the opposing party on the grounds that the production of private information would violate the Stored Wire and Electronic Communications Privacy Act (SCA). The SCA prohibits electronic

communication services from disclosing the contents of its subscribers' communications expect where a specific, narrowly defined exception exists. Many commentators have questioned whether this 25-year old law is adequate to handle today's technology, but the courts are nonetheless finding that it does apply to social media discovery.

In *Crispin v. Christian Audiger, Inc.*,[8] the court granted reconsideration of a Magistrate Judge's decision to deny Plaintiff's motion to quash subpoenas issued to several social networking sites that sought disclosure of Plaintiff's subscriber information and communications relevant to the underlying dispute. Of particular importance, the court analyzed the applicability of the Stored Communications Act (SCA) to the social networking sites at issue. Here, the court noted provisions of the SCA applied to "providers" of communication services and the information they possess concerning entities and individuals.[9] For information to be afforded protection from disclosure under the SCA, a provider must either be an "ECS" or a "RCS" provider.[10] As pointed out by the court, the SCA has defined an ECS provider as any service which provides its users the ability to send or receive wire or electronic communications. Conversely, the court explained that the statute has defined a RCS provider as "the provision to the public of computer storage or process services by means of an electronic communications system and deserving of a lesser standard of protection concerning communications."[11]

Applying these definitions in the instant case, the court found that all of these social networking sites qualified as an ECS provider because they provided message delivery services, and also as a RCS provider because they offered message storage services.[12] As an interesting

---

[8] 2010 WL 2293238 (C.D. Cal. May 26, 2010).
[9] *Id*. at 4.
[10] *Id.*
[11] *Id.*
[12] In support of its conclusion, the court cited examples of ECS, including basic e-mail services and private electronic bulletin board services. Further, the court recognized that an RCS provider offered

aside, some have posited that because electronic communications typically combine both services – message delivery and message storage – the ECS and RCS definitions in the SCA may have become a distinction without a difference.

After determining the SCA to be applicable, the court then turned to whether the information requested in the subpoena was public or private; the latter of which is protected from disclosure by the SCA while the former is not. The court in *Crispin* held that the Web mail and e-mail communications sought were inherently private because these messages were not readily accessible to the public or, at most, were only available to a select few individuals. As such, the court reversed the Magistrate Judge's order with respect to the social networking subpoenas to the extent that they sought private e-mail messages. However, with respect to the Facebook wall postings and MySpace comments, the court determined that there was not enough evidence on record to make a determination as to whether these wall postings and comments constituted private communications. Accordingly, the court ordered a new evidentiary hearing regarding those portions of the subpoenas that sought Facebook wall postings and MySpace comments.

The court's holding appears to appreciably restrict a civil litigant's ability to obtain potential evidence that can only be described as a proverbial "smoking gun" by extending the protections of the SCA to private communications sent through a social networking or web hosting site. Moreover, the 1986 law doesn't "fit" very well in the modern content – the court seems to be hammering a square peg in a round hole. How many "friends" are on the "private" part of a social media site before the distinction between public and private is lost, especially where all the friends are free to do whatever they want with the content? Since the case was one of first impression, the decision is not binding on other courts. It will be interesting to see how

---

longer-term storage or processing services, more or less like a virtual filing cabinet. Finally, the court noted that Microsoft was an example of both an ECS and RCS because it provided both e-mail delivery and storage services through its Hotmail website.

other courts react – and it would be helpful if Congress would retool a law whose time is long gone.

HURDLES TO ADMISSION: AUTHENTICATING THE EVIDENCE

Once an attorney has jumped the first hurdle and obtained some relevant information from a social networking site, the next hurdle that he or she must surmount is actually admitting that information into evidence. Fortunately, courts have provided some guidance into the issues that may arise here. For the most part, the courts have been fairly consistent in applying the traditional rules of evidence in this area, albeit, there have been some notable exceptions worth mentioning.

One feature that draws many individuals to social media sites and to the Internet generally is the level of anonymity; anyone can set up an account under a false name, and information on a "legitimate" site can be manipulated. This feature, however, has given attorneys countless evidentiary headaches and courts have responded by requiring electronic evidence to be authenticated prior to being admitted in evidence. Generally speaking, many courts have required that the party seeking to admit such evidence provide evidence such that a reasonable jury could find that the exhibit is what the party claims it to be. Importantly, the court in *State v. Bell*,[13] specifically pointed out that the evidentiary support necessary for admissibility was "quite low." There, the court admitted several MySpace entries, finding sufficient authentication included testimony from the proponent that: (1) he had knowledge of defendant's e-mail address and MySpace user name, (2) the printouts appeared to be accurate records of his electronic communications with defendant, and (3) the communications contained code words known only

[13] 882 N.E.2d 502 (2008)

to defendant and his alleged victims. Likewise, in *Griffin v. State*,[14] the Maryland Court of Special Appeals permitted an anonymous MySpace page to be admitted to show that a key witness had been intimidated into changing his story. In so holding, the court explained that social media profiles on MySpace and Facebook could be authenticated circumstantially by their content and context in the same manner as other forms of electronic communications.

With that in mind, the admission of social media evidence becomes much easier when there is any admission from the witnesses, or at least an admission by the plaintiff or witness of the IP address along with the IP logs that should be produced by the social networking sites. Most courts have followed a common sense, requiring rigorous authentication only if someone disputes the legitimacy of the evidence. It is always wise to make a Request for Admissions, file Stipulations, etc. so that all of these issues are resolved before trial.

SOCIAL MEDIA AND JURORS

At least one state court has held that attorneys can research prospective jurors using social media in the courtroom during jury selection. Internet research and access to social media has the potential for opening up a whole new avenue to excuse a juror for cause. Specifically, a lawyer might be able to determine from social media activity that a juror is not being candid or truthful in his or her response to questions. In addition, periodic checks during trial might provide evidence that a juror is engaging in outside research, contacting witnesses or even the individual on trial, or commenting about their premature verdict in this case. Each of these scenarios has actually occurred.

[14] 995 A.2d 791 (Md.App., 2010).

As to juror questioning, the case of *State v. Dellinger*,[15] is illustrative. There, juror Amber Hyre did not disclose that she had knew the defendant and that she had actually sent him a message between receiving her jury summons and appearing for jury duty. On appeal, Dellinger argued that the juror's lack of candor on *voir dire* supported his request for a new trial. The court agreed and reversed the trial court and ordered a new trial. Of particular importance, the appellate court concluded that "the totality of Juror Hyre's responses during the June 11, 2008, coupled with her repeated silence during *voir dire*, leads this Court to conclude that she had such connection with Appellant and witnesses…that bias must be presumed." Perhaps social media research could have revealed juror Hyre's connection to the defendant in the first instance, thereby saving valuable time and money spent arguing the issue on appeal and the subsequent new trial.

Social media juror monitoring shouldn't stop there. Attorneys should ask the court to have the jury list any blogs or Web sites for which they post on a regular basis. Attorneys should then check those sites during the trial and after to ensure that no juror has breached his or her legal obligations. For instance, diligent social media research has uncovered many a juror posting comments about the case or his or her verdict prior to the case's completion. In fact, a juror posted details on a case on her Facebook page and polled her online friends on how the case should be decided. Similarly, a juror decided to announce on Facebook how fun it was going to be to "tell the defendant they're GUILTY." Mind you, this was posted *before* the defendant put on her case. In addition, there have been cases where individuals have tampered with the jury through social networking sites. In one such case, the girlfriend of a California defendant tried to influence the jury's decision using MySpace. The list of questionable conduct by jurors literally goes on and on.

[15] 696 S.E.2d 38 (2010).

Fortunately, lawyers and courts are getting smarter. Courts today, on their own accord or at the request of counsel, usually instruct a jury and litigants that they are not to use social media to discuss the case, to research the case, or to friend parties to the litigation. Many states have even adopted instructions that specifically address and prohibit the use of social media during trial. There is a new proposed federal court instruction designed to do the same thing.

CONCLUSION

Litigators are wily. Once they discover a new tool for their arsenal, they are quick to adopt it. 80% of family lawyers report seeing a sharp rise in the use of social media evidence in divorce cases. Though the reported cases addressing the legal issues of using of social media evidence are relatively few, the use of such evidence "in the wild" is growing rapidly.

In the next couple of years, we anticipate a growing body of case law – along with a lot of professional tips from lawyers who are increasing savvy about getting and using social media evidence. In the litigator's toolkit, social media comes with a skimpy book of instructions – but the length of the book is growing exponentially each year.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, computer forensics and information security firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com