Searching Social Networking Sites

Investigators can use information gleaned from social media, but the Bar and the law have strict rules about it.

By Deborah A. Lujan

Investigators and adjusters today are asking a common question: Is information on social networking sites useful for lawyers and investigators? The answer is yes, but obtain and use with caution.

In 2010, Facebook surpassed Google as the most popular website, according to Experian Hitwise. Facebook reports that it currently has over 800 million users. User pages often contain photos, videos, messages, and a list of friends; thus, it is likely that access to claimant, witness or employee pages will reveal valuable information.

This information can be helpful in preparing for depositions, mediation and trial, even if not ultimately admissible—inadmissible evidence can lead to the discovery of admissible information. But issues may arise in connection with the access to, and use of, information published through social networking sites.

Public vs. Private Information and the Federal Stored Communications Act

An issue to consider is user privacy interests. If a person's Web page is open to Internet users indiscriminately, there is generally no expectation of privacy. In *Moreno v. Hartford Sentinel, Inc.*, the court found no reasonable expectation of privacy in an article the user posted on MySpace because it was "available to any person with a computer." In *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, the court stated that "[t]he privacy concerns are far less where the beneficiary herself chose to disclose the information."

However, many social networking sites contain "private" information that is unavailable to the public. Additionally, a user can send private messages to others through the websites. The Stored Communications Act (SCA) is a federal statute that prohibits third parties from accessing private electrically stored communications without proper authorization. Specifically, an offense is committed if anyone: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access a facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system…." Note that the SCA does not apply to an "electronic communication [that] is readily accessible to the general public."

The SCA may prevent providers of electronic communications from complying with a civil subpoena for a user's private information. For example, courts have held that the SCA prohibits providers, such as Google Mail and Yahoo Mail, from releasing the contents of a customer's e-mail account (see *Bower v. Bower*). In *Crispin v. Christian Audigier, Inc.*, the court quashed subpoenas to Facebook and MySpace, holding that some of the content hosted on their sites is protected under the SCA; i.e., private messages sent through the sites were "inherently private" because they were not readily accessible to the general public.

But some courts, without addressing the SCA, have held that social networking sites must divulge information pursuant to a civil subpoena. In *Ledbetter v. Wal-Mart Stores, Inc.*, the court found that subpoenas to Facebook, MySpace and Meetup.com that sought information about the personal injury plaintiffs were relevant and reasonably calculated to lead to the discovery of admissible evidence.

Ethical Considerations

If a lawyer is prohibited from engaging in contact with a claimant, so is a private investigator or third party. Attorneys can be disciplined for getting a third party to "friend" a witness or claimant on a social media site. State and national bar association rules of professional conduct prohibit attorneys from engaging in activities that could be viewed as dishonest or fraudulent or that are a misrepresentation. They prohibit an attorney from making a false statement of material fact to a third person, and they prohibit communicating with persons known to be represented by counsel.

However, in York City Bar Opinion 2010-2, the ethics committee concluded that an attorney "may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request. While there are ethical boundaries to such 'friending,' they are not crossed when an attorney or investigator uses only truthful information, subject to compliance with all other ethical requirements." In Philadelphia Bar Association Ethics Op. 2009-02 (March 2009), the committee stated that a lawyer may "forthrightly" ask an unrepresented person for access to his social networking site, but the lawyer's agent cannot make that same contact because the unrepresented person might be more likely to grant access to someone he does not associate with the lawyer and, thus, be deceived.

In *Barnes v. Cus Nashville, LLC*, the court indicated that it was willing to create a Facebook account and send a friend request to the plaintiffs "for the sole purpose of reviewing photographs and related comments in camera" and then "disseminat[ing] any relevant information to the parties."

Admissibility Issues – The Bottom Line for Use

The rules of evidence govern the admissibility of information from social networking sites. Like all evidence, the proponent has to demonstrate that it is relevant. The court may conduct an *in camera* review to make this determination. Its probative value must outweigh the danger of unfair prejudice, confusion and misleading the jury.

There are also issues of hearsay, as noted in *Maldonado v. Municipality of Bareceloneta*. In *Miles v. Raycom Media, Inc.*, the court stated: "Because the Facebook page and the comment to the article constitute unsworn statements made by third parties that are offered to prove the truth of the matter asserted, they constitute inadmissible hearsay…." However, the contents of a social networking site may be admissible under the rule providing that admissions of a party-opponent are non-hearsay. In *Telewizja Polska USA, Inc v. Echostar Satellite*, the court held that archived contents of a skinhead organization's website that posted the name, address and picture of the victim, along with a call to attack him, "may be considered an admission of a party-opponent, and are not barred by the hearsay rule."

Several other hearsay exceptions may apply, such as a "statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter" (Fed. R. Evid. 803(1)). Consider also Fed. R. Evid. 801(21), "reputation of a person's character among associates or in the community."

Social media must be properly authenticated. In *Griffin v. State*, the court held that a MySpace page wasn't properly authenticated because the prosecutor didn't ask the witness if the page was hers and if she had authored the contents. The picture of the witness on the page, her birth date, and her location were not enough given the "potential for abuse and manipulation of a social networking site by someone other than its purported creator."

Fed. R. Evid. 901 provides that the requirement of authentication "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Tips for authenticating information from social networking sites include providing testimony of the person who created the Web page; information regarding when and how the Web page was created and/or maintained; affirming that printouts from the website provided are accurate (i.e., accurate to what appeared on the Internet); and/or subpoenaing the material directly from the source.

Deborah A. Lujan and **Tracey M. Bobo** are attorneys with Southfield, Mich.-based *Collins, Einhorn, Farrell & Ulanoff, P.C.* www.CEFLawyers.com