Utilizing Social Media in Litigation

By Rick Conner

"The future ain't what it used to be" – Yogi Berra

The world is changing, and litigators must stay abreast of new developments and adapt their practices to fit the new reality of the electronic age. Mailed letters and faxes are becoming a thing of the past as the world moves toward speedier forms of communication such as emails, text messages, and social media posts. The explosion of social media has created a bounty of new information that attorneys cannot afford to ignore. Instead, litigators must understand how to find and preserve social media evidence and get it admitted in a lawsuit.

According to *Digital Insights*, there are currently more than 1.15 billion total users on Facebook; more than 500 million users on Twitter; more than 500 million users on Google+; more than 238 million users on LinkedIn; more than 130 million users on Instagram; and more than 70 million users on Pinterest. Harsh Ajmera, *Social Media facts, figures and statistics 2013* (modified September 4, 2013) ***http://blog.digitalinsights.in/social-media-facts-and-statistics-2013/0560387.html***. On average, more than 400 million tweets are sent every day. *Id.* More than half of all Americans have a profile on a social networking site. Tom Webster, *The Social Habit*, June 2012, ***http://socialhabit.com/secure/wp-content/uploads/2012/07/The-Social-Habit-2012-by-Edison-Research.pdf***. Nearly two-thirds of social network users utilize social network sites on a daily basis. *Id.* In such a world, ignoring social media evidence places an impediment on the search for truth. Kathrine Minotti, *Evidence: The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. Rev. 1057, 1074 (2009).

Social media can be a rich source of background information for litigators preparing to depose a witness, and is being used increasingly as substantive or impeachment evidence in federal and state court cases. Profile pages, wall posts, photographs, chat transcripts, and private messages can all have potentially major evidentiary impacts in a lawsuit. For example, in one New York case, the plaintiff in a personal injury lawsuit claimed that she had sustained severe and permanent injuries that left her largely bedridden. The court granted the defendant's motion for access to the plaintiff's MySpace and Facebook accounts because of pictures that allegedly showed the plaintiff smiling happily outside the home after the alleged injury. **Romano v. Steelcase Inc.**, 907 N.Y.S.2d 650, 654 (N.Y. App. Div. 2010). Additionally, in one North Carolina case, the Court of Appeals ruled that evidence on a minor's social media page, including suggestive photos and indications that she was not a virgin, was admissible for impeachment purposes in a custody proceeding brought by the county against her father based upon allegations of rape and abuse. **In the Matter of K.W.**, 192, N.C. App. 646, 666 S.E.2d 490, 494 (2008).

This article discusses considerations for the collection and preservation of social media evidence, how the rules of civil procedure and rules of evidence address social media evidence, and the admissibility of social media evidence in litigation.

Collection and Preservation

Social media evidence is more likely to be admitted at trial when it has been properly obtained. H. Christopher Boehning and Daniel J. Toal, *Authenticating Social Media Evidence*, Volume 248, No. 65, New York Law Journal (Oct. 2, 2012). One of the best ways to obtain the evidence is for the account holder to download the relevant materials from the social media website. Facebook, for example, has a page that assists users in downloading information from your online profile. *Downloading Your Info* (modified July 2013) ***https://www.facebook.com/help/131112897028467***. It is also relatively simple to do a printout, screen capture, or use an archive tool to capture information, but these methods will not capture all associated metadata. To collect metadata associated with social media information, attorneys should consider hiring e-discovery experts who have specialized collection tools and experience in collecting such data. Boehning and Toal, *supra*.

Collecting data from social media sites can raise ethical concerns, however. For example, is it ethical for an attorney to contact a Facebook friend of an opposing party in order to request access to the Facebook page of the opposing party? Is it ethical for an attorney to ask a legal assistant to send a friend request to a witness so the attorney can access his or her Facebook profile? Simply researching a witness's social media public profiles should be permissible, but ethics rules may prohibit using deception in order to obtain access to social media profiles. Thomas Spahn, *The Ethics of Email and Social Media* (modified April 17, 2013) ***http://www.alanet.org/conf/2013/handouts/LI31_The_Ethics_of_Email.pdf***. These ethical issues have not yet been addressed by the North Carolina State Bar or the Attorney General's office.

Attorneys must also make sure to craft their litigation hold notices to include social media evidence and advise their clients against deleting social media posts and messages that relate to the lawsuit. Deleting relevant social media posts can lead to spoliation claims and sanctions. For example, in a personal injury action in federal court in New Jersey, the defendants asked the court to impose sanctions against the plaintiff for failing to preserve his Facebook account. The court ruled that it would be appropriate to give a jury instruction allowing an adverse inference against the plaintiff for deleting his Facebook account. **Gatto v. United Air Lines, Inc.**, No. 10-cv-1090-ES-SCM, 2013 WL 1285285 (D. N.J. Mar. 25, 2013). In another case, a Virginia judge ordered a plaintiff's attorney to pay $542,000 for instructing his client to remove photos from his Facebook profile, and ordered the client to pay an additional $180,000 for obeying the instructions. The attorney was afraid that pictures from his client's Facebook account would prejudice his wrongful death case based upon his spouse's fatal automobile accident. For example, one of the photos showed the widower holding a beer and wearing a t-shirt that said "I [illegible text] hot moms." John Patzakis, *Facebook Spoliation Costs Lawyer $522,000; Ends His Legal Career*, Next Gen. eDiscovery L. & Tech. Blog (November 5, 2011), ***http://blog.x1discovery.com/2011/11/15/facebook-spoliation-costs-lawyer-522000-ends-his-legal-career/***.

Attorneys who send subpoenas to social media providers such as Facebook and Twitter must be wary of the Stored Communications Act ("SCA"). 18 U.S.C. § 2701 et. seq. The SCA was originally adopted in 1986 to protect privacy interests in personal and proprietary information that may be stored on the Internet. Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 Harv. J.L. & Tech. 563, 565-566 (2011). Congress has not updated the statute since 1986, however, and courts have struggled with how to apply the SCA to today's technologies. *Id.* at 566. The SCA applies to communications stored on the internet by third-party providers, including social media providers like Facebook and LinkedIn. *Id.* at 567. The SCA cannot be used by an individual to defeat a court order requiring the individual to produce content from his or her social media profiles, but is often cited by social media providers like Facebook and MySpace as grounds for refusing to comply with subpoena. *Id.*; *see also Juror Number One v. Superior Court*, 142 Cal. Rptr. 3d. 151, 158-159 (Cal. Ct. App. 2012) (holding that even if a juror's Facebook postings are protected by the SCA, that protection applies only to attempts to compel production from Facebook and not to attempts to compel production by the juror).

The SCA protects communications stored by electronic communications services ("ECS") and remote computing services ("RCS"). *Id.* The SCA defines an ECS to be "any service which provides to users thereof the ability to send or receive wire or electronic communications," and defines an RCS to be a provider of "computer storage or processing services by means of an electronic communications system." 18 U.S.C. §§ 2510(15) and 2711(2). The SCA generally protects RCS and ECS providers from having to disclose the electronic communications of users to the government or a third party without a search warrant. Ward, *supra* at 568. The restrictions apply only to content information contained in electronic communications, and likely do not extend to things like a social network user's user name or account activity data. *Id.* The SCA also only prohibits ECS and RCS providers from disclosing content information that is held for certain specific purposes. *Id.* at 569.

The first court to extend protection to social networks under the SCA was the United States District Court for the Central District of California in **Crispin v. Christian Audigier, Inc.** 717 F. Supp.2d 965 (C.D. Cal. 2010). In **Crispin**, the court ruled that Facebook and MySpace were ECS providers because they provided message delivery services, and were also RCS providers because they offered message storage services. *Id.* at 985-987. The court relied on the SCA in quashing subpoenas for the plaintiff's private messages sent through Facebook and MySpace because they were private electronic communications. *Id.* Regarding Facebook wall posts and MySpace comments, the court ruled that these posts and comments would be protected by the SCA only if they were not "completely public," and remanded the case to the magistrate judge to determine whether the plaintiff's privacy settings rendered the wall posts and comments public or private. *Id.* at 981, 991.

One author recommends a two-step approach for courts in ruling on challenges to subpoenas to social media providers: (1) determine whether the request is both narrowly tailored to produce relevant information and reasonably calculated to lead to the discovery of admissible evidence, and (2) determine whether the SCA protects the requested information from disclosure. Ward, *supra* at 582.

Applicable Rules of Civil Procedure and Evidence

Neither the North Carolina nor the Federal Rules of Civil Procedure specifically address social media evidence, so courts are left to apply the existing rules of civil procedure to the discovery of evidence from social media sites. Both the North Carolina Rules and the Federal Rules, however, have rules regarding "electronically stored information" ("ESI"). The North Carolina Rules of Civil Procedure allow discovery of ESI on the same basis as other types of documents, but allow for a party to make additional objections to the production of such data if the ESI is from a source that the party identifies as not reasonably accessible because of undue burden or cost, or if the requested form of production is unreasonable. N.C.R.Civ.P. 26(b) and 34(b). The Federal Rules of Civil Procedure similarly allow discovery of ESI on the same basis as other types of documents, and allow for similar objections. Fed.R.Civ.P. 26(b)(2)(b) and 34(b)(2). Although the rules don't specifically define ESI to include social media, some commentators have opined that courts should treat social media evidence as ESI because (1) the Federal Rules Advisory Committee intended the rule on ESI to be flexible; (2) social media website components are similar in structure and function to traditional forms of ESI (like e-mail); and (3) case law on traditional forms of evidence provides guidance for any differences between social media websites and other forms of ESI. Minotti, *supra* at 1062-1063 (2009).

Similarly, neither the Federal Rules of Evidence nor the North Carolina Rules of Evidence specifically address electronic data or social media information as a distinct category of evidence. Instead, federal courts and North Carolina courts apply the traditional rules of evidence in determining the admissibility of social media evidence. Challenges to social media evidence usually come in the form of hearsay objections or objections based on the proffering party's failure to properly authenticate the evidence. *Id.* at 1066.

A recent North Carolina Court of Appeals decision shows how powerful social media evidence can be in a case when it gets admitted. A murder suspect told police that he was in Philadelphia at the time of the crime, and that his Facebook page would verify his claim. **State v. Chaplin**, 753 S.E.2d 397, No. COA13-393, 2013 WL 5947754, *5 (N.C. Ct. App. Nov. 5, 2013). When a detective checked his page, he saw a status update three days before the crime indicating the defendant was in Philadelphia. *Id.* However, Facebook's records, which were admitted into evidence, showed that the update had been posted from an IP address in Greensboro that was associated with an unsecured wireless network owned by a man who lived next to one of the defendant's friends. *Id.*

Authentication and Admissibility

In order to get social media evidence admitted in a legal proceeding, remember the acronym OPRAH:

- **O** – Original writing rule
- **P** – Probative value substantially outweighs the danger of unfair prejudice
- **R** – Relevance
- **A** – Authenticity
- **H** – Hearsay and exceptions.

Cheryl Howell, UNC School of Government, *Electronic Evidence Issues*, ***http://www.sog.unc.edu/sites/www.sog.unc.edu/files/HowellElectronicEvidenceHandout.pdf*** (last edited April 2010) (giving credit for this acronym to Durham attorney Donald Beskind); see also **Lorraine v. Markel American Ins. Co.**, 241 F.R.D. 534, 538 (D. Md. 2007). In many cases, the greatest challenge regarding admissibility of social media evidence is authentication – the remainder of this article therefore focuses on that element.

Rule 901(b) of the Federal Rules of Evidence and the North Carolina Rules of Evidence both provide illustrative lists of methods by which evidence can be authenticated. According to United States District Court Judge Paul Grimm (District of Maryland), who authored a benchmark decision for social media evidence in **Lorraine v. Markel American Insurance Company**, *supra*, the authentication rules most likely to apply to social media evidence are Rules 901(b)(1) (testimony of a witness with knowledge); 901(b)(3) (comparison with an authenticated document); 901(b)(4) (distinctive characteristics); 901(b)(7) (evidence about public records); 901(b)(9) (evidence about a process or system); and 902(5) (official publications). Paul W. Grimm, Lisa Yurwit Bergstrom, and Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. 433, 464 (2013).

For example, a person who created a social media page can testify to its authenticity under Rule 901(b)(1). A "unique speech pattern" coupled with knowledge of occurrences that only a few people would have known about can sufficiently authenticate a post on a social media website under Rule 901(b)(4). **Campbell v. State**, 382 S.W.3d 545, 551-552 (Tx. Ct. App. 2012). A combination of photographs, video, comments, e-mail addresses, posting dates, metadata, and IP addresses, if they provide enough content and context, can also be sufficient for circumstantial authentication. Boehning, *supra* at 2. Other circumstantial evidence that courts may look to in determining whether an Internet posting has been authenticated include:

> The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities … whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question.

Minotti, *supra* at 1067-1068 (citing **Lorraine**).

There are two inconsistent lines of cases regarding authentication of social media evidence. One line of cases sets a high bar for admitting social media evidence by holding that such evidence should not be admitted unless the court has definitely determined that the evidence is authentic. Grimm, *supra* at 441; see also **Griffin v. Maryland**, 19 A.3d 415 (Md. 2011). The second line of cases takes a different approach and decides the admissibility of social media evidence based on whether there is sufficient evidence of authenticity for a reasonable jury to conclude that the evidence is authentic. *Id.*; see also **Tienda v. Texas**, 358 S.W.3d 633 (Tex. Crim. App. 2012). If the proponent produces sufficient evidence to convince a reasonable juror that the social media evidence is authentic, the burden shifts to the objecting party to prove facts demonstrating that the putative creator of the social media evidence did not in fact create the evidence. *Id.* at 456. If the court finds that a reasonable juror could find for either the proponent of the evidence or for the party objecting to the evidence, then the trial judge admits the evidence conditionally and allows the jury to determine whether to accept or reject the evidence. *Id.*

Judge Grimm believes the approach adopted in this second line of cases is better reasoned based on the interplay of Rules 104(a) and (b), Rule 901, and Rule 401. *Id.* Judge Grimm states that a judge should admit social media evidence if there is plausible evidence of authenticity produced by the proponent, and only speculation and conjecture – not facts – presented by the opponent about how, or by whom it might have been created. *Id.* at 459. Under this approach, "clearly authentic evidence is admitted, clearly inauthentic evidence is excluded, and everything in between is conditionally relevant and admitted for the jury to make the final determination as to authenticity." *Id.* at 465.

For example, in **New York v. Clevenstine**, the state offered into evidence instant messages exchanged on MySpace between the defendant and the victims he allegedly raped. The defendant objected claiming that the evidence had not properly been authenticated. 891 N.Y.S.2d 511 (N.Y. App. Div. 2009). The appellate court found that the trial court properly admitted the MySpace messages because: (a) the victims testified that they had engaged in messaging through MySpace with the defendant about sexual activities; (b) an investigator testified that he had retrieved these messages from the hard drive of the computer used by the victims; (c) a legal compliance officer from MySpace testified that the messages had been exchanged by users of accounts created by the defendant and the victims; and (d) the defendant's wife recalled the sexually explicit conversations she viewed in the defendant's MySpace account while on their computer. *Id.* at 514. The court acknowledged that it was possible that someone else could have accessed the defendant's MySpace account and sent the messages under his name, but determined that the trial court "properly concluded that, under the facts of this case, the likelihood of such a scenario presented a factual issue for the jury." *Id.*

It does not appear that North Carolina courts have expressly weighed in on which approach they will follow in the admission of social media evidence, but judging from handouts that the UNC School of Government provides to district court judges (see Rubin, *supra*, noting that Howell's handout is provided to district court judges). North Carolina courts will likely follow the second approach favored by Judge Grimm. Howell, *Electronic Evidence Issues*, *supra*, Note 37 at p. 2 ("proponent does not need to rule out all possibilities inconsistent with authenticity, or to prove beyond a reasonable doubt that the evidence is what it purports to be"); see also **Horne v. Vassey**, 157 N.C. App. 681, 579 S.E.2d 924 (2003) ("Authentication does not require strict, mathematical accuracy, and a lack of accuracy will generally to go the weight and not the admissibility of the exhibit").

Judge Grimm suggests the following checklist for practitioners looking to authenticate social media evidence:

1. Prior Preparation – Plan for the introduction of social media evidence at trial while engaging in discovery, and ask questions of deposition witnesses that will lay the appropriate foundation under Rules 901(b) and 902.
2. Do Your Homework – Know whether the judge or court presiding over your case has issued any opinions on the admissibility of social media evidence and adapt your approach accordingly. If you are asking the court to change its prior view, file a motion in limine well before trial to get an advance ruling.
3. Ask for a Stipulation or Admission – Opposing counsel may very well stipulate to the authenticity of the evidence that you are seeking to introduce, or admit the authenticity of the evidence in response to a Rule 36 request for admission.
4. Remember the Interplay of Rules 104(a) and (b) and "Conditional Relevance" – If you are aware of facts that your adversary will attempt to prove to rebut the evidence you intend to offer to authenticate your social media evidence, consider whether you can argue that the facts offered by your adversary are insufficient to convince a reasonable jury that your evidence is not authentic.
5. Plan the Method of Introduction – Determine in advance of trial the rule or rules you are planning to use to authenticate the social media evidence.
   Grimm, *supra*, at 466-468.

Conclusion

As social media becomes more pervasive in our society through new users and new platforms like Instagram and Pinterest, litigators should recognize and embrace the vast amounts of personal information and potential evidence that social media may offer. Attorneys must carefully consider how to preserve and collect relevant social media evidence, how to gear their discovery strategy toward laying a foundation for authentication, and how to get social media evidence admitted at trial. Careful planning at an early stage in a case can help to ensure that valuable evidence is not lost or overlooked and will not be excluded at trial.

Rick Conner is Counsel at McGuireWoods LLP in Charlotte, North Carolina.