Chapter Thirteen

Social Media

David J. Walton
Jason A. Cabrera
Jessica Hurst

13-1 INTRODUCTION

Social media use has grown increasingly popular in recent years, with Facebook alone now claiming more than 1.1 billion active users worldwide. Facebook, YouTube, LinkedIn, and Twitter are four of the top ten most popular websites in the United States. The Pew Research Center reports that 66 percent of all adults in the United States with Internet access use at least one of the various social media platforms. Even though social media use is predominantly with younger users, use among those aged 50 or older nearly doubled in 2010. With the ubiquity of social media, an increase in discovery requests and litigation surrounding it was inevitable. This chapter will explore some basic concepts surrounding social media, when social media evidence could be available in litigation, and ways to use social media evidence in practice.

13-2 BASIC CONCEPTS/SOURCES OF SOCIAL MEDIA

A complete list of the sources of social media is practically impossible; every year seemingly produces yet another set of social media companies marketing their brands to the public. We will recount here the major players, up-and-coming companies, and make note of other sites to watch.

13-2.1 Major Players

The major players in the social media category all share similar characteristics: major usage among Americans, widespread brand recognition, the sharing of personal data, ideas, or observations, and the ability to broad-

cast content directly to the public at large. Obviously, many companies will satisfy all these categories, but the most prominent of them are described below.

Facebook has long been the dominant social media company in the world and, although perhaps difficult to believe, will celebrate its 10-year anniversary in 2014. Although most of Facebook's recent growth has been outside the United States, more than 133 million Americans have a Facebook account and it is the second most-visited website in the United States (after Google). Facebook profiles contain spaces for a virtual treasure trove of personal information including name, birthday, names of friends, status messages from the user, photos, places recently visited, relationship status, the ability to "like" a post by a friend or colleague, and much more. Facebook reports that its users are uploading 350 million new photos each day, making it the largest photo-sharing site in the world.

YouTube, the main online video clearinghouse owned by Google, is the third most-visited website in the country. LinkedIn, a prominent networking tool that is geared toward professional contacts, Twitter, a social networking and microblogging platform, and Pinterest are all in the top 12 most-visited websites in the United States. MySpace, one of the first social networking sites, has decreased in popularity, but may provide information on those users who still maintain pages. Blogs, which provide a personal online platform for individuals or companies, are still popular websites, though not nearly as widespread as the other sources mentioned above. Together, these websites represent the most popular social networking vehicles and a potential source of valuable personal information about parties and witnesses that may be useful in litigation.

13-2.2 Up-and-Coming Sites

Social media start-ups are frequent, but some companies have stood above the rest of the pack and it may be important to consider them when considering the discovery possibilities of social media. Streaming video is becoming easier to access and sharing photos is a common use of social media platforms. In addition to YouTube, other sites in this category include Instagram, which allows users to create profiles, share pictures, and follow their friends; Tumblr, which permits the posting of a variety of materials by users and also permits a user to subscribe to accounts of their friends or others; Flickr and Picasa, photo sharing sites; and Vine, where users can upload 10-second video clips and easily post links to them on other social media sites. Depending upon the specific factual situation in an individual case, these sites could provide access to evidence (photos, videos, etc.) that would otherwise be difficult to learn about or to obtain. Another similar (and very popular) mechanism is Snapchat, an app for smartphones that permits photos to be shared among certain friends, but

the photo is automatically deleted after it is viewed. Snapchat is probably less susceptible to discovery methods given that the company doesn't usually store the transferred content in its servers, but its popularity suggests it should not be overlooked.

13-2.3 Other Sites

Other sites with more niche communities may still provide plenty of information. Reddit, which has a mostly male and younger user base, is still in the top 30 most-visited sites in the country. Pinterest, which has a mostly female user base, launched in 2010 and by mid-2012 registered 25 million unique visitors in a single month (overtaking Tumblr). FourSquare provides a location-based check-in service, with users incentivized to "check in" and register their location. A listing of these additional sites could continue for a while and yet still be incomplete. Practitioners should cast a wide net in discovery for all types of social media sites—the major players, up-and-coming sites, smaller online communities, and the sites in the future that are sure to be developed.

Practice Tip: Remember that courts tend to view unlimited demands to view an entire social media account or every social media account a person maintains with suspicion; make sure that the discovery requests can be properly supported or tailored to the issues actually in litigation.

13-3 WHEN IS SOCIAL MEDIA EVIDENCE AVAILABLE: DISCOVERY

The advent of social media has greatly expanded the body of discoverable information in litigation. Yet, despite its novelty, courts generally apply basic discovery principles to the discovery of social media content. Thus, social media is discoverable to the extent that it is relevant and the requests are not unreasonably annoying, oppressive, or embarrassing. See, e.g., *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566 (C.D. Cal. 2012). The user's right to privacy is generally not an acceptable defense to discovery requests for social media content. See, e.g., *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650 (N.Y. 2010) ("[A]s neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy"). Even "private" or "locked" social network content will be discoverable in appropriate circumstances. See, e.g., *Equal Empl. Opportunity Comm'n v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010) ("[A] person's expectation and intent that her communications

be maintained as private is not a legitimate basis for shielding those communications from discovery"); *Romano*, 907 N.Y.S.2d at 657 ("[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 settings"). However, despite the inapplicability of the privacy defense, a requesting party will generally not have free reign to access the user's entire social network profile. See, e.g., *Tompkins v. Detroit Metro. Airport*, 278 F.R.D 387, 388 (E.D. Mich. 2012) ("[T]he Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public view"); *Howell v. Buckeye Ranch, Inc.*, Civil Action 2:11-cv-1014 (S.D. Ohio October 1, 2012) ("The fact that the information defendants seek is an electronic file as opposed to a file cabinet does not give them the right to rummage through the entire file"). But see section 13-3.2 below regarding Pennsylvania state courts granting full access to social media content.

13-3.1 Requested Content Must be Relevant

Ultimately, a party requesting social media content will only be permitted to access that content accessible under the general discovery rules—that which is "reasonably calculated to lead to the discovery of admissible evidence." See, e.g., *Tompkins*, 278 F.R.D. at 388. In *Trail v. Lesko*, an Allegheny County Common Pleas judge noted that the courts of common pleas in Pennsylvania follow a consistent approach and "recognize the need for a threshold showing of relevance prior to discovery of any kind, and have nearly all required a party seeking discovery in these cases to articulate some facts that suggest relevant information may be contained within the non-public portions of the profile." *Trail v. Lesko*, No. GD-10-017249 (C.P. Allegheny July 3, 2012).

13-3.1.1 Demonstrating Relevance Through Publicly Accessible Content

Often, relevancy may be demonstrated by showing that publicly accessible information on a party's social network site controverts his or her claims or defenses. For example, in *Thompson v. Autoliv ASP, Inc.*, the plaintiff alleged that she suffered "massive, life-threatening, permanent, and irreversible injuries" resulting from a vehicular collision, including stroke, paralysis of the right side of her body, intensive speech therapy, permanent scarring and disfigurement, and the need for extensive physical rehabilitation and psychological and emotional counseling. *Thompson v. Autoliv ASP, Inc.*, 2:09-cv-01375-PMP-VCF (D. Nev. June 20, 2012). The plaintiff also alleged that she lost the quality and enjoyment of her life because she was restricted in engaging in most physical activities, experienced an in-

crease in emotional distress, and would be limited in her ability to care for her children if and when she had them. The plaintiff sued the manufacturers of the seatbelt and airbag systems in her vehicle.

One of the defendants conducted informal discovery (see section 13-3.3 below on informal discovery) of the public portions of the plaintiff's Facebook profile and obtained wall posts and photographs depicting the plaintiff's ability to dance, swing on a swing set, engage in water sports, and care for children and pets, as well as the plaintiff's social activities including late-night partying and consumption of alcohol. Public portions of her profile also depicted the plaintiff's personal relationships, post-accident recovery, her employment, and the effect of her medications on her emotional, physical, and sexual habits. The court held that evidence relating to the plaintiff's social activities and physical capabilities was relevant to her claimed injuries. As a result, the court ordered the plaintiff to provide the defendants with an electronic storage device containing all information from her Facebook and MySpace accounts so that defense counsel could identify discoverable material that the plaintiff had previously withheld.

Several Pennsylvania courts have also found the relevance requirement to be established via public postings. See *Brogan v. Rosenn, Jenkins & Greenwald, LLP*, 28 Pa.D.&C.5th 553 (C.P. Lackawanna 2013) ("[A] party may obtain discovery of private Facebook posts, photographs and communications only if the electronically stored information is relevant, and the party may satisfy that relevancy requirement by showing that publicly accessible information posted on the user's Facebook page controverts or challenges the user's claims or defenses in the pending litigation"); *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535 (C.P. Northumberland May 19, 2011) (public portion of plaintiff's social media profiles negated plaintiff's allegations regarding his alleged injuries); *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD (C.P. Jefferson September 9, 2010) (a review of the public portion of plaintiff's Facebook page revealed posts showing plaintiff may have exaggerated his injuries, which made the remaining contents of plaintiff's Facebook page relevant).

Practice Tip: Conduct informal discovery of public portions of a social media profile, or propound specific interrogatories regarding social media evidence before requesting access to an individual's social media account.

13-3.1.2 Alternative Ways to Demonstrate Relevance

As an alternative to showing relevant information on a public profile, parties may also be able to propound specific interrogatories and requests for production of documents to determine if relevant information exists on an individual's social networking profile. See, e.g., *Largent v. Reed*, No. 2009-1823 (C.P. Franklin November 8, 2011); see also *Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc.*, Case No. 2:06-cv-00788-JCM-GWF (D. Nev. January 9, 2007) (noting that defendants should make more specific discovery requests for social media, but not mentioning any initial showing of relevance through the user's public posting). Relevance may also be shown by referring to relevant content on another party's page. See, e.g., *Equal Empl. Opportunity Comm'n v. Original Honeybaked Ham Co. of Georgia,* Civil Action No. 11-cv-02560-MSK-MEH (D. Colo. November 7, 2012) ("Given the fact that Defendant has already obtained one affected former employer's Facebook pages, and that those pages contain a significant variety of relevant information, and further, that other employees posted relevant comments on this Facebook account, I agree that each class member's social media content should be produced").

13-3.1.3 Annoyance, Embarrassment, Oppression

Finally, closely related to the relevance inquiry is the question of whether the discovery request will cause unreasonable annoyance, embarrassment, or oppression. For example, in *Trail v. Lesko*, the Allegheny County Court of Common Pleas considered the discovery of Facebook posts to be intrusive because the opposing party would gain access to information that had little to do with the litigation. The court explained that the discovery would be barred by Pa.R.C.P. 4011 if the seeking party could not show that the discovery would result in relevant evidence. However, the court also noted that Facebook discovery rated a 2 on an intrusiveness scale of 1 to 10 because the Facebook user already voluntarily made the information available to a number of people with no legal obligation to keep the information confidential. For a level 2 intrusion, the party seeking discovery "needs to show only that the discovery is reasonably likely to furnish relevant evidence, not available elsewhere, that will have an impact on the outcome of the case." The court thus denied the parties' cross motions to compel access to each other's Facebook accounts because the discovery intrusions "were not offset by any showing that the discovery would assist the requesting party in presenting its case."

13-3.2 Discovery Requests Should Be Narrowly Tailored

In many cases, a court will not permit a party to have access to an entire social network account, and courts typically reject such requests as fishing expeditions. See, e.g., *Tompkins*, 278 F.R.D. at 388 (holding that a defen-

dant is not permitted "to engage in the proverbial fishing expedition, in the hope that there *might* be something of relevance in Plaintiff's Facebook account"); *Mackelprang*, Case No. 2:06-cv-00788-JCM-GWF ("Ordering Plaintiff to execute the consent and authorization form for release of all of the private email messages on Plaintiff's Myspace.com internet accounts would allow Defendants to cast too wide a net for any information that might be relevant and discoverable").

To overcome the courts' prohibition against "fishing expeditions," requests for social media discovery must be narrowly tailored. For example, in *Mackelprang*, the plaintiff sued her former employer for sexual harassment, alleging that she had been diagnosed with post-traumatic stress disorder, depressive disorder, and panic disorder stemming from her intolerable work environment. The plaintiff also alleged she attempted to commit suicide as a result of the conditions of her working environment. The defendants requested that the plaintiff sign a "consent and authorization for private messages" on the plaintiff's two MySpace accounts, and filed a motion to compel when the plaintiff refused to comply. The defendant requested access to the plaintiff's MySpace messages because they could have contained "statements made by Plaintiff and witnesses about the subject matter of this case" and "information that Plaintiff's alleged severe emotional distress was caused by factors other than Defendant's alleged sexual harassment misconduct." The court refused to order the plaintiff to execute the consent form because access to all of the plaintiff's private messages "would allow Defendants to cast too wide a net for any information that might be relevant and discoverable." The court advised the defendants that the proper way to obtain social media content from the plaintiff would be "to serve upon Plaintiff properly limited requests for production of *relevant* email communications," that is, "private messages that contain information regarding her sexual harassment allegations in this lawsuit or which discuss her alleged emotional distress and the cause(s) thereof."

Even when a claimant alleges mental or emotional health injuries, a request for social network posts relating to "any emotion" may be too broad. See, e.g., *Mailhoit*, 285 F.R.D. at 572 (seeking communications relating to "any emotion" could be understood to require production of posts such as "I hate it when my cable goes out"). But see *Simply Storage Mgmt., LLC*, 270 F.R.D. at 436 (ordering plaintiff to respond to a similar request and produce "any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and [social media] 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 a significant emotion, feeling, or mental state").

As one Court of Common Pleas judge noted, Pennsylvania is distinguishable from other jurisdictions in that other jurisdictions "have wrestled to establish a middle ground between the wholesale denial of the request on the one hand and the granting of unlimited access to the user's profile on the other." *Trail v. Lesko*, No. GD-10-017249 (C.P. Allegheny July 3, 2012). In contrast with the national trend, Pennsylvania state courts have actually granted access to social network accounts carte blanche. See, e.g., *Mazzarella v. Mount Airy Casino Resort*, No. 1798 CV 2009 (C.P. Monroe November 7, 2012) (granting motion to compel log-in and password without threshold showing of relevance); *Gallagher v. Urbanovich*, No. 2010-33418 (C.P. Montgomery February 27, 2012) (granting motion to compel defendant's Facebook log-in and password for seven-day period without any threshold showing of relevant information in public profile); *Largent v. Reed*, No. 2009-1823 (C.P. Franklin November 8, 2011) (plaintiff's public profile fulfilled relevance requirement so court ordered plaintiff to produce login and password for 21-day period); *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535 (C.P. Northumberland May 19, 2011) (ordering plaintiff to produce his passwords, user names, and log-ins for Facebook and MySpace with no time limitation).

Practice Tip: Narrow requests for social media content as it relates to relevant issues are more likely to be upheld than broad requests for "all social media content" within a given time frame.

13-3.3 Whether to Conduct Formal or Informal Discovery

Discovery of social media may be conducted formally or informally. Parties may follow the formal route of propounding interrogatories regarding an individual's use of social networking sites, or ask the party about social network use during a deposition. Interrogatories should ask the respondent to identify every social networking site he or she has used within the relevant time frame, and to identify the Web addresses, usernames or e-mail addresses, and other registration information associated with the accounts. In an effort to obtain information showing that the social network profile is relevant to the litigation, the requesting party should include interrogatories regarding whether the user's social network profile contains any posts, pictures, etc. concerning the issue at hand (for example, emotional state, injury, social life, quality of life, etc.). A party can also ask these questions during a deposition.

Parties can then follow up with document requests for the actual social media content. The document requests should include not just requests for current information on the social media account, but for any changes or

updates to the account in the relevant time frame. The document requests should be broad enough to include the wide array of posts that may be made on social media sites, including pictures, private messages, status updates, tagged posts, etc. All of the requests should be narrowly tailored for specific information that makes clear the relevance of the information to the litigation.

Parties may also conduct informal discovery of social media, but must be mindful of both the authentication (see section 13-4.2 below) and ethical issues that may arise as a result. To conduct informal discovery, search each social networking site to determine the extent of the individual's social media presence. Search engines such as Google will also reveal what information is available about an individual online. Most often, informal discovery will only lead to publicly available information on a user's profile. Parties may have to eventually resort to formal discovery to access private portions of social media accounts, given the ethical concerns that arise when attempting to informally discover private content.

Informal discovery of private social media content has been addressed by several ethics committees. Some states hold that attorneys may send friend requests to unrepresented parties, provided they identify themselves. For example, the New York City Bar Association Committee on Professional Ethics considered the question of whether a lawyer may resort to trickery via the Internet, that is, creating a fake profile, to gain access to a social networking page. NYC Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2010-2. The committee answered that question in the negative, and concluded that such activity would be in violation of Rule 8.4(c) of the New York Rules of Professional Conduct, which prohibits a lawyer from engaging in conduct involving dishonesty, fraud, deceit, or misrepresentation, and Rule 4.1, which prohibits a lawyer from knowingly making a false statement of fact or law to a third person. Id. However, the committee did conclude that "an attorney or her agent 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." Id.

However, the Pennsylvania bar takes a less lenient approach than New York, and would likely find that friend requests to non-party witnesses must reveal the intent behind the request. In 2009, a lawyer wanted to enlist a third party to friend-request a non-party witness. The Philadelphia Bar Association concluded that the proposed course of conduct violated Pennsylvania Rule of Professional Conduct 8.4, which, like New York's Rule 8.4, prohibits lawyers from engaging in conduct involving dishonesty, fraud, deceit, or misrepresentation. Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02. The committee found the proposed conduct unethical

because the third party, although being truthful about his identity, would not reveal to the witness that he intended to obtain information for use in a lawsuit to impeach the witness's testimony. Id.

Problems will also arise when a lawyer openly sends a friend request to a represented party. In San Diego, a plaintiff filed a wrongful discharge action against his former employer, and the plaintiff's attorney sent friend requests to high-ranking employees of the employer. The San Diego Legal Ethics Committee concluded that the plaintiff's attorney had participated in unethical ex parte contact with a party. San Diego Cnty. Bar Legal Ethics Comm., Op. 2011-2. The committee considered the high-ranking employees to be part of the "corporate party," and sending friend requests to them was equivalent to communicating directly with a party an attorney knows to be represented, in violation of California Rule of Professional Conduct 2-100. In line with Philadelphia, the San Diego committee also determined it to be unethical for the lawyer to send a friend request to a represented party without disclosing why the request was sent. The committee did note, however, that nothing would prevent the attorney's client from sending a friend request to an opposing party.

13-3.4 How Social Media is Produced

Outside of Pennsylvania state court, given the limitation on "fishing expeditions," parties will usually only be required to produce specific content, rather than password or log-in information that would give the requesting party unfettered access to a social network account. See, e.g., *Howell v. Buckeye Ranch, Inc.*, Civil Action 2:11-cv-1014 (S.D. Ohio October 1, 2012) ("Howell's username and password would gain defendants access to all the information in the private sections of her social media accounts—relevant and irrelevant alike"). But see section 13-3.2 above for Pennsylvania cases in which log-in information is ordered to be produced.

Alternatively, some courts will conduct an in camera review and determine which social media information should be produced. See *Offenback v. L.M. Bowman, Inc.*, Civil Action No. 1:10-CV-1789 (M.D. Pa. June 22, 2011) (court ordered plaintiff to provide log-in information and reviewed plaintiff's Facebook and MySpace profiles to determine which portions of plaintiff's profile were relevant); *Original Honeybaked Ham Co. of Georgia,* Civil Action No. 11-cv-02560-MSK-MEH (requiring class of plaintiffs to produce their social media content in camera based upon defendants' showing that one plaintiff's Facebook page contained relevant evidence, and appointing a special master to collect the evidence).

13-3.4.1 Production Format

Once a document request is granted, social media content may be produced electronically, as actual documents, or in rarer instances, complete access may be granted to the social media account (see section 13-3.2 above). Some social media sites allow users to download their own information. For example, Facebook provides users the option to "download a copy of your Facebook data" under "Settings." Data that can be downloaded include posts on the account and posts made to others' accounts, photos, photo metadata, deleted friends, searches made on Facebook, status updates, account history, changes made to the "About" section of the account, any items hidden from the user's news feed, IP address, date and time associated with each log-in and log-out of Facebook, etc. As another example, on Twitter, users can click on "Settings" and request their Twitter archive dating back to the beginning of their account.

Practice Tip: If authentication is expected to be an issue, requesting the metadata associated with the social media content (for example, log-in information or IP addresses) will be key.

13-3.5 Obtaining Discovery from the Social Media Site

If obtaining social media records from a party fails, seeking to subpoena them directly from the social network site will likely be unsuccessful. In *Crispin v. Christian Audigier, Inc.*, the court held that private messages on a Facebook and MySpace account were protected by the Stored Communications Act (SCA), 18 U.S.C. § 2701(a)(1). *Crispin v. Christian Audigier, Inc.,* 717 F.Supp.2d 965, 991 (C.D. Cal. 2010). The SCA protects private electronic communications and sets limits on when a communications service provider can disclose user information depending upon whether the provider provides electronic communication services (ECS) or remote computing services (RCS). In *Crispin*, defendants in a breach of contract and copyright infringement action served a subpoena *duces tecum* on MySpace and Facebook seeking the plaintiff's communications with another individual. *Crispin*, 717 F.Supp.2d at 968–69. The court in *Crispin* determined that Facebook and MySpace could qualify as either ECS or RCS, and quashed the subpoena for private messages. See 18 U.S.C. § 2510(15); *Crispin*, 717 F.Supp.2d at 980, 990. The court further held that wall posts may also be protected from disclosure by the SCA depending upon the user's privacy settings, and suggested that the SCA would protect such wall posts if the user limited public access to his or her postings. *Crispin*, 717 F.Supp.2d at 991.

In light of the SCA, most social network sites only permit parties to request basic subscriber information, and not any private content. For example, Facebook permits parties to a civil action to request "basic subscriber information (not content)" only if "1) the requested information is indispensable to the case and not within the party's possession; and 2) you personally serve a valid California or federal subpoena on Facebook. Out-of-state civil subpoenas must be domesticated in California and personally served on Facebook's registered agent." http://www.facebook.com/help/205949546109965. Facebook requires the user's e-mail address, Facebook user ID, and vanity URL. Names, birthdays, locations, and other information are insufficient to identify a Facebook account.

Social network sites will produce user content if the user signs a consent and authorization form for its release. See 18 U.S.C. § 2702(b)(3); *Romano*, 907 N.Y.S.2d at 657 (ordering plaintiff to produce a properly executed consent and authorization as may be required by the operators of Facebook and MySpace). Although such an authorization may be unnecessary for websites like Facebook, which enables users to download a copy of their own Facebook data, it may be necessary to obtain less accessible information such as metadata, deleted friends, deleted posts, etc.

Practice Tip: Obtain the user's consent before requesting discovery directly from the social media site.

13-3.6 Preventing Users from Deleting Their Social Media Account

Finally, it is worth noting that, as with other forms of discovery, attorneys should ensure that the opposing party takes precautions to preserve the contents of their social media accounts. For example, Facebook notes on its Help page that information a user deletes from his or her account is deleted from Facebook servers. https://www.facebook.com/help/www/405183566203254. Similarly, many users may be quick to delete information from their social media website upon learning of pending litigation. Thus, it is important to issue preservation notices as soon as possible.

13-4 WAYS TO USE SOCIAL MEDIA EVIDENCE IN THE LAW

Once social media evidence has been obtained in a given case, the next question becomes how to *use* that evidence to your advantage in a hearing/trial itself. Although most lawyers are familiar with the general rules regarding authentication and hearsay, social media evidence presents unique challenges as courts adapt longstanding interpretations to new

technology. This section will discuss ways to use social media evidence in the law and present tips and pointers where you can learn about common examples that may help you in your practice.

In 2007, a federal magistrate judge issued a lengthy opinion that set forth the major evidentiary principles regarding the admission of electronic evidence. *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007). The judge described the process of admitting electronic material into evidence as being determined by "a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible." Id. at 538. The judge categorized the hurdles as relevance, authenticity, hearsay, best evidence, and unfair prejudice. Id. Each hurdle is addressed below as a separate section.

13-4.1 Relevance

Relevance is a most basic evidence rule and does not have any special characteristics when applied to social media evidence. The general definition from the federal rules—that relevant evidence means evidence having "any tendency to make a fact more or less probable than it would be without the evidence" and that "the fact is of consequence in determining the action"—will apply and practitioners will generally not face any special challenges in proving the relevance of social media evidence in a given case.

13-4.2 Authentication

The focus of any discussion on authentication begins with Federal Rule of Evidence 901. The general rule announced in Rule 901 is that the proponent of evidence must "produce evidence sufficient to support a finding that the item is what the proponent claims it is." This standard rule is applicable even when facing the challenges posed by social media evidence. See *In re F.P.*, 878 A.2d 91, 95 (Pa.Super. 2005) ("We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa.R.E. 901"). But this standard doesn't provide much guidance to practitioners faced with social media evidence. Rule 901(b) provides a list of examples of evidence that meets the authentication standard, and lawyers faced with the need to authenticate social media evidence at trial must attempt to use the examples in 901(b) as much as possible.

Before a discussion of the 901(b) factors, however, a quick note about Rule 104 and the standards for conditional relevancy is necessary. Essentially, the judge makes the *initial* determination about the authenticity of electronic evidence pursuant to Rule 104(a), requiring the proponent to offer a satisfactory foundation from which the jury could reasonably find the evi-

dence is authentic. Then the jury will ultimately make any necessary factual findings to determine authenticity under Rule 104(b), using evidence presented to them during trial. *Lorraine*, 241 F.R.D. at 539–40.

13-4.2.1 Easy Cases: Testimony of Witness Who Drafted the Evidence in Question

The easiest method of authentication is by testimony from a witness with knowledge that the identified item is what it claims to be. If you need to authenticate an e-mail or a text message, the testimony from the person who drafted that e-mail or text message would likely be sufficient. Some questions you may be able to ask the witness to authenticate electronic evidence he or she created would be:

- Who created the file/electronic evidence?
- Where was the file stored?
- How do you know the file is in its original form?
- Who had access to the file?
- Did anyone edit the file?

The appropriate answers to these questions from your witness should satisfy the 901(b)(1) standard. If your only witness is someone with personal knowledge about how ESI is generated, the testimony of that person may just be enough if the witness can provide factual specifics about the process of creating or storing the ESI without alteration. See *Lorraine*, 241 F.R.D. at 555–56.

13-4.2.2 Harder Cases: Comparisons

If you are left without the testimony of the person who drafted the message, but you still have some messages from the purported author that are beyond question, you can use the comparison method in 901(b)(3) to authenticate the messages.

Under Rule 901(b)(3), either a trier of fact or an expert may compare a purported exhibit with "an authenticated specimen." If the trier of fact concludes that the exhibit is similar enough to the authenticated specimen given, then the trier of fact can conclude that the exhibit is genuine. For example, a jury can compare an e-mail (E-mail A) with other e-mails that have already been produced and authenticated (E-mail B) and then conclude that E-mail A is similar enough to E-mail B to authenticate E-mail A.

Practice Tip: The comparison method of authentication was successfully used by the government in a 2006 criminal case. *United States v. Safavian*, 435 F.Supp.2d 36 (D.D.C. 2006).

13-4.2.3 Distinctive Characteristics

Federal Rule of Evidence 901(b)(4) describes how distinctive characteristics—"appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances"—satisfy the authentication requirement.

Under this rule, parties may find that the e-mail address or screen name, content with which the proponent is familiar, or testimony by a witness to whom the party spoke about the subject matter of the e-mail would be sufficient under 901(b)(4) for authentication. See *United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000).

Many types of electronic evidence have "metadata" that can be helpful to establish ownership or control. Metadata includes details about a file's name, location, format, type, size, date, and permissions; metadata is typically created without input from the user and can be a distinctive characteristic sufficient to authenticate data containing it. Sometimes metadata is stored inside attached files, so it may be available even if the person who drafted the e-mail or attachment is not available to authenticate it. Hash marks are also incredibly useful tools that may be available. Hash marks provide a unique numerical identifier to a file, inserted into the original electronic document when it is created to provide it with a distinctive character sufficient for 901(b)(4) authentication purposes.

13-4.2.4 Computerized Public Records

Public records have long been authenticated under Rule 901(b)(7), which permits authentication for evidence that a document was recorded or filed in a public office as authorized by law or for evidence that a purported public record or statement is from the office where items of that kind are kept. This rule will permit the authentication of computerized public records, such as tax returns, social security records, correctional records, etc.

To use the second prong of this authentication method, the proponent must show that the office from which the records were taken is the legal custodian of them. *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 548 (D. Md. 2007). This step isn't as difficult as it may sound. A certificate of authenticity from the office or the testimony of an official who is autho-

rized to testify as to custodianship is fine. Even testimony from a witness with knowledge that the records are from a public office that is authorized to keep such records may be enough.

13-4.2.5 Computer-Generated Records

How do you handle computer-generated records where there is no individual who "made" the record or has sufficient personal knowledge to testify about the underlying facts? The procedure in 901(b)(9) may be helpful for your purposes. Rule 901(b)(9) permits "[e]vidence describing a process or system and showing that it produces an accurate result." For electronic evidence generated by a computer or other electronic process, evidence it produced will be authenticated if a proponent can show the data input procedures and the accuracy of those procedures, as well as evidence that the computer was routinely tested for programming errors that could have affected the accuracy of the results.

13-4.3 Hearsay

Hearsay is likely the largest obstacle to the admission of social media evidence. But the well-known rule has multiple avenues that a litigator can use to limit its application and admit social media evidence that might initially appear to run afoul of the general prohibition on the admission of out-of-court statements offered for their truth.

Before addressing the common exclusions and exceptions that may apply, first examine whether the evidence in question even meets the definition of hearsay in the first place. In order to be "hearsay," the evidence must be (1) an oral or written assertion or nonverbal conduct if intended by the person to be an assertion, (2) made by a person, and (3) offered in evidence to prove the truth of its content. If the evidence does not meet all three prongs, then it fails to meet the definition of hearsay and would not be excludable under the hearsay rule.

13-4.3.1 Computer-Generated Content Has No Declarant and Is Not Hearsay

In *Lorraine*, a federal magistrate judge held that electronically generated records entirely the product of a computerized system or process were not hearsay because they were not made by a person. The example the judge used was of a report generated when a fax is sent that showed the fax number of the recipient and the time the fax was sent. Since "there is no 'person' involved in the creation of the record, and no 'assertion' being made," the record fails to meet the definition of hearsay because there was no declarant—that is, no person who made the statement.

Multiple courts have used the same logic to admit electronic evidence that might at first glance appear to be inadmissible hearsay. The Third Circuit, regarding the admission of a fax record in *United States v. Khorozian*, 333 F.3d 498 (3d Cir. 2003), held that the header on the fax was not hearsay because "a statement is something uttered by 'a person,' so nothing 'said' by a machine . . . is hearsay." A federal magistrate in Illinois upheld admission of a printout of a website from an Internet archive, offered to show what the website in question looked like on particular dates in the past. The proponent of the evidence supplied an affidavit from the Internet archive company that verified the company retrieved from its archives the copies of the website that were offered. The court found that the printouts were not "statements" as defined by the hearsay rule. *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.,* Case No. 02 C 3293 (N.D. Ill. October 15, 2004). An appeals court in Mississippi found an automatic e-mail generated by a Facebook messaging system that contained both the underlying message and confirmation that the message was received was not hearsay for lack of a declarant or an assertion. *Smith v. Mississippi*, No. 2012-KA-00218-COA (Miss. App. June 4, 2013).

13-4.3.2 Proving the Truth of the Matter Asserted

Out-of-court statements are still not hearsay if the proponent is not offering them to prove the truth of the underlying matter. Litigators should examine whether they need to offer social media evidence for its truth or if the evidence is actually needed for a different purpose. In *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000), the government offered into evidence e-mails between the defendant and his co-worker. The Eleventh Circuit noted that those e-mails were not hearsay because they were admitted to show the relationship of the two individuals and their custom of communicating by e-mail. Id. at 1323. And the traditional examples of evidence not offered for its substantive truth—verbal acts, to show the effect on the listener of the statement, questions, or imperative commands—are all still applicable to social media evidence.

13-4.3.3 Common Exclusions from Hearsay Rule

Some evidence that meets the three prongs of the hearsay definition—that it was a statement, made by a person, and offered for its substantive truth—might nevertheless still be excluded from the hearsay rule under F.R.E. 801(d). That rule excludes from hearsay two types of evidence: certain prior statements by witnesses who actually testify and are subject to cross-examination, and five types of party-admissions that are offered against a party.

The most well-known aspect of this rule is the party-admission exclusion found in F.R.E. 801(d)(2). (In Pennsylvania, the party-admissions exclusion is listed instead as an exception to the hearsay rule, Pa.R.E. 803(25), though the text is nearly identical and the different placement is not intended to have substantive effect.) This section excludes from the definition of hearsay any statement that is offered against an opposing party and was made by the opposing party, by a person authorized by the opposing party to make a statement on the matter, by the opposing party's agent or employee concerning a matter within the scope of agency or employment, by an opposing party's co-conspirator in furtherance of the conspiracy, or was a statement in which the opposing party manifested its adoption or belief that the statement was true.

Statements in social media and electronic evidence have often been found to be excluded as party admissions by federal judges. E-mails authored by a party are often the easiest to qualify, but a federal district court also held e-mail sent by employees of the defendant (when offered against the defendant) as party admissions. See *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146, 1155 (C.D. Cal. 2002).

13-4.3.4 Common Hearsay Exceptions

Evidence that has not been found admissible at this stage of the review qualifies as hearsay and is inadmissible unless one of the exceptions found in Federal Rules of Evidence 803, 804, or 807 apply. (Note that Pennsylvania has not adopted the residual hearsay exception found in F.R.E. 807). Although nearly 30 exceptions to the hearsay rule exist under those three rules, only a handful of them are commonly used regarding social media evidence. This section will focus its attention on those more common examples, all of which are found in F.R.E. 803.

Federal Rules of Evidence 803(1) and (2) provide exceptions to the hearsay rule for the present-sense impressions made while the declarant was perceiving the event or for excited utterances made while the declarant was under the stress or excitement of a qualifying condition. These exceptions will be most helpful with social media evidence that recounts a person's impressions, thoughts, or perceptions of an event then-occurring. Twitter feeds, status updates on Facebook, and similar media that provide outlets for users to convey current plans, locations, or observations are especially fertile grounds for the use of F.R.E. 803(1) and (2) exceptions.

Evidence of a declarant's then-existing state of mind is an exception to the hearsay rule under F.R.E. 803(3), as long as the state of mind is relevant to an issue in the case. Social media evidence will often contain the impressions, feelings, emotions, and motives of the author, so F.R.E. 803(3) will be a particularly useful avenue for admission of hearsay evidence.

Business records are excepted from the hearsay rule under F.R.E. 803(6), but this exception requires a significant amount of foundation that may be lacking for social media evidence. To qualify for this exception, evidence must (1) be prepared in the normal course of business, (2) be made at or near the time of the event it recorded, (3) be based on the personal knowledge of the person who made the entry or someone who had a duty to convey the information to the person who entered it, (4) be made in the regular course of a regularly conducted business activity, and (5) must have been the regular practice of the business to make the record, all as testified to by a custodian or other qualified witness (or pursuant to a certification under F.R.E. 902(11)). Courts have taken a varied approach to how to handle F.R.E. 803(6) exceptions for social media evidence, from strict scrutiny of each prong to relatively lenient standards without critical analysis, and practitioners should be prepared to defend any business records assertion as much as possible.

Practice Tip: For examples of a strict approach to the business records exception, look at *Rambus, Inc. v. Infineon Techs. AG*, 348 F.Supp.2d 698 (E.D. Va. 2004). For examples of a more lenient approach, read *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000).

13-4.4 Best Evidence

The complicated structures of the rule commonly known as the best evidence rule can be summarized rather simply: the rule applies only when a proponent seeks to prove the content of a writing, recording, or device; duplicates are as admissible as originals unless there is a genuine concern about the authenticity of the duplicate; and secondary evidence about the contents of a writing, recording, or photograph are permitted if all originals and duplicates have been lost without bad faith, are otherwise unobtainable, the opponent has the original and won't produce it, or it relates to a collateral matter. Printouts for electronically stored information are originals pursuant to F.R.E. 1001, but social media evidence is quite susceptible to loss or destruction, so practitioners should be aware of this evidence hurdle and the ways to avoid being trapped by a best evidence objection.

13-4.5 Unfair Prejudice

Federal Rule of Evidence 403 provides for the exclusion of relevant evidence under certain circumstances, such as confusion of the issues, misleading the jury, or when its probative value is substantially outweighed

by the danger of unfair prejudice. The rule is used sparingly, but may be an appropriate vehicle to exclude certain types of inflammatory social media evidence.

A special note is necessary about computer-generated images or animation, which are particularly susceptible to a Rule 403 objection. Computer-generated animation was first approved for use in a Pennsylvania criminal case, despite objections that the evidence was unfairly prejudicial to the defendant, by the Pennsylvania Supreme Court in 2006. *Commonwealth v. Serge*, 896 A.2d 1170 (Pa. 2006). The Supreme Court noted that the absence of sounds, facial expressions, evocative movements, and other factors demonstrated the animation scene was not unduly prejudicial, though it did recognize the inflammatory nature of a computer-generated animation scene that purported to represent how a murder was conducted. Although a 2011 opinion from the court upheld the use of a clip from *America's Most Wanted* in a defendant's criminal trial, the court was "deeply troubled" by its use; the court reinforced the importance of the limiting factors used in the *Serge* animation, and upheld the use of the clip mostly due to the waiver of objection and acceptance of the trial court's limiting instructions. See *Commonwealth v. Maisonet*, 31 A.3d 689 (Pa. 2011). Although computer-generated animation can be appropriate in an individual case, litigators would be wise to closely follow the parameters approved in *Serge* to minimize the likelihood that a Rule 403 objection would be successful.

13-5 NEXT BIG THING

As smartphones become more prevalent and powerful and wireless connectivity becomes more widespread, the next big thing in the social media world will likely involve location-based services. Apple announced its new location-based app, iBeacon, with the introduction of its new operating system, iOS 7. Several major American companies—Starbucks, Macy's, American Airlines, and Major League Baseball—have agreed to test the product in some locations. The theory behind iBeacon is that a collection of tiny beacons at a store or location would be used to pinpoint the location of a user's phone; when a user reaches a certain location in the store or area, a message could be sent directly to their phone. The possibilities for use are endless; perhaps a coupon after a user's tenth visit to the store, or a welcome message, or any number of other messages that would be useful to a consumer or business. Both Apple and the companies involved are concerned about the privacy of users in this upcoming feature and both are treading lightly to avoid discouraging users from the service. Nevertheless, location-based services have the potential to offer new benefits to users, a new platform for companies, and have enormous potential for growth.

13-6 CONCLUSION

In the end, the only thing constant about social media is that the medium is always changing. Facebook started in 2004 as a small project open only to about 20,000 students at Harvard University; ten years later, over 1 billion people have a Facebook account. Twitter started in mid-2006 and, six years later, its users were submitting 340 million tweets *per day*. Snapchat began in 2011 and, just two years later, it rejected a $3 billion offer from Facebook to buy the company and a Pew Research Center survey reported nearly 10 percent of the United States cell phone market (26 million users) had Snapchat accounts. The next big thing on the social media scene isn't yet widely known and may not even be developed yet, but the safe assumption is that a new product will eventually be marketed to the public that may change the way we connect with each other online.