Investigative Techniques Using Advanced Technology

By Michael A. McCaskey, William E. McDonald III, and Charles Smith

Now more than ever, it is crucial for attorneys to become familiar with the various investigative techniques for locating and accessing this information.

As information shared across the internet and social media became more pervasive over the last decade, information created, shared, and saved on the internet began making its way into legal proceedings across the nation.

Now, as technology evolves, the next iteration of user-generated data has surfaced. Correspondingly, the availability of online investigative and preservation techniques has become increasingly prevalent. Social media platforms allow users to create and share increasing amounts of personal information, while more and more connected devices enable users to generate and share data in real time and on location. As of the spring of 2015, 72 percent of all American adults owned and used a smartphone. This percentage jumps to 83 percent for American adults between the ages of 30 and 49; for the coveted 18- to 29-year-old group, the share jumps even higher, to a whopping 86 percent. Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, Pew Research Ctr. (Feb. 22, 2016), *available at* http://www.pewglobal.org.

Following this trend, Facebook reports more than 1 billion monthly active users. Justin Kerby, *Here's How Many People Are on Facebook, Instagram, Twitter, and Other Big Social Networks*, Adweek (Apr. 4, 2016), *available at* http://www.adweek.com (last visited Oct. 18, 2016). And Twitter has an estimated 500 million registered users. *Id.*

Social media use is growing three times quicker than overall internet use, and its popularity continues to grow. *The State of the Media: The Social Media Report 2012*, Nielsen, *available at* http://blog.nielsen.com. Now more than ever, it is crucial for attorneys to become familiar with the various investigative techniques for locating and accessing this information. Equally impor-



■ Michael A. McCaskey is a partner in the Chicago office of Swanson Martin & Bell LLP. His national litigation practice includes representing clients in matters involving product liability, catastrophic injury, toxic tort, and commercial litigation. Mr. McCaskey currently serves as the DRI Automotive SLG marketing chair. William E. McDonald III is an associate at Bush Seyferth & Paige in Troy, Michigan, where he focuses his practice on commercial and product liability litigation, financial services litigation, and trademark enforcement. Charles Smith is an associate in McGlinchey Stafford's New Orleans office, where he handles primarily automotive product liability matters.

tant is the need to understand how this information can be used for, and against, clients in legal proceedings.

By capturing available information early, defense counsel are in a better position to compel additional social media evidence from a resisting plaintiff, as demonstrated in *Richards v. Hertz Corp.*, 100 A.D.3d 728, 953 N.Y.S.2d 654, 656–57 (N.Y. App. Div. 2012). There, the court ordered an *in camera* inspection of "all status reports, emails, photographs, and videos posted on [plaintiff's] Facebook profile since the date of the subject accident to determine which of those materials, if any, are relevant to her alleged injuries." *Id.* This followed only after the defendants demonstrated that the plaintiff's otherwise private Facebook page contained one photograph that was relevant to the injuries claimed. *Richards,* 100 A.D.3d at 730, 953 N.Y.S.2d at 654.

Some courts may even require a preliminary social media investigation before ordering production of a plaintiff's private social media information. In *Arcq v. Fields*, No. 2008-2430 (Pa. Com. Pl. Franklin Cnty. Dec. 8, 2011), the court denied the defendant's motion to compel access to the plaintiff's private Facebook profile because the defendant could not show a "good-faith belief" that the plaintiff's private profile would reveal relevant information. The public portion of the plaintiff's Facebook profile, which the court considered to be "a gateway to the private profile," did not reveal any relevant information that would give rise to the conclusion that the private profile would lead to admissible evidence. *Id.* at 3–4.

Conducting a thorough and up-front online investigation helps to shape the discovery plan and support the request for additional discovery as a case evolves.

Authenticating Internet and Social Media Evidence

One explanation of the etymology of the saying "a little bird told me so" is that it originates in the use of carrier pigeons. For nearly 2,000 years the carrier pigeon was used to communicate critical military and political messages. The risk associated with using a carrier pigeon was that it was susceptible to being intercepted by enemies who could change the message to their advantage before releasing the pigeon to its intended recipient. Therefore, a system of unique markings was developed to ensure that the message received was, in fact, authentic and correct. In its simplest terms, admitting web evidence in court requires a similar process of verifying authenticity, typically through metadata (*i.e.*, data about data) unique to each piece of web evidence. In light of the sheer volume of online data and the availability of image-altering software, web evidence has become increasingly scrutinized by American courts. Practitioners should be familiar with the methods and options to authenticate web evidence. Requesting the admission of such evidence without the proper authentication is otherwise akin to requesting admission because "a little bird told me so."

Common Practice Pitfalls

One common practice made by many attorneys is simply to print the desired online evidence and place it in a file, or to take a "screenshot" of the evidence and save it as a .pdf document to a local hard drive. Such a practice can be fraught with practical and evidentiary challenges. A screenshot alone may be insufficient to meet the authenticity requirement, and some courts have rejected mere printouts. For example, a Kansas district court held that "[a screen capture] fails to identify who retrieved the website printout, when and how the pages were printed, or on what basis the printouts accurately reflect the contents of the website on a certain date." *Toytrackerz v. Koehler*, 2009 WL 2591329, at *6 (D. Kan. Aug 21, 2009). Similarly, in *Linscheid v. Natus Medical, Inc.* No. 3:13-cv-76-TCB, 2015 WL 1470122 (N.D. Ga. Mar 30, 2015), the court found that a printed LinkedIn webpage was not properly authenticated by a declaration from the individual who merely printed the webpage. The Second Circuit also found that the testimony of an investigator who printed a defendant's social media page was insufficient to authenticate the web evidence. *United States v. Vayner*, 769 F.3d 125, 131 (2nd Cir. 2014).

Therefore, practitioners should expect, and be prepared to meet, increasingly strict admissibility standards. In general, the authentication concerns expressed by courts fall into three categories. First, appearance is important. Quite often the standard "screen print" has a drastically different appearance compared to the actual website. This can be due to printer formatting or website multimedia software such as Adobe Flash. A printout with a distorted appearance alone may be enough for a court to be skeptical about admitting the evidence. Second, a prudent opponent may argue that the availability of image-editing software allows screen-printed web evidence to be altered with ease, thus undermining the reliability of the tendered document. Third, the internet is ephemeral by its very nature; website content can change daily, if not by the minute or second. Therefore, a proponent may have a difficulty proving that the "evidence is what it purports to be" when tendering a printed image of a website that no longer exists or has changed by the time of trial.

Some courts may even require a preliminary social media investigation before ordering production of a plaintiff's private social media information.

How would courts view web evidence as properly preserved and authenticated so that it can be admitted at trial, months or perhaps years after it is collected? Some courts have required the proponent of the web evidence to produce the underlying metadata as a prerequisite to admissibility. Common metadata for a website may include the website address (URL), IP address, source file (DOM and HTML), browser type, and operating system. The next section will analyze the authenticity requirements for web evidence under the Federal Rules of Evidence and provide some practical tips for collecting and protecting the admissibility of it.

Admissibility Requirements for Web Evidence: Relevancy and Authenticity

As with other evidence, web evidence must be relevant and authenticated to be admis-

sible. Relevancy is governed by Federal Rules of Evidence 401 and 403, and authentication is governed by Federal Rule of Evidence 901. Generally, proponents of web evidence should be prepared to provide the metadata (to prove that the evidence is what the proponent claims), and be able to show that the web evidence was securely stored since it was collected (chain of custody). Therefore, practitioners should be mindful of the available authentication methods for web evidence. If at all possible, authentication issues should be addressed before trial, either through a request for admission or pre-trial stipulation. Third-party software, as discussed below, is also a practical and useful method to address authentication concerns.

As with other evidence, web evidence must be relevant and authenticated to be admissible.

To establish authenticity under Federal Rule of Evidence 901, the proponent of the evidence "must produce evidence sufficient to support a finding that the item is what the proponent claims." Fed. R. Evid. 901(a). Federal Rule of Evidence 901(b) provides a non-exhaustive list of evidence that satisfies the Rule 901(a) authentication requirement. Although not conclusive, the general methods in Federal Rule of Evidence 901(b) provide a useful framework to analyze admissibility of web evidence, specifically those listed in 901(b)(1), (3), (4), and (9).

Under 901(b)(1), authenticity is established through testimony of a witness with knowledge that an item is what it is claimed to be. In the context of web evidence, the 901(b)(1) method may include calling a witness who collected the web evidence. Ideally, this witness would have recorded when and where the web evidence was collected, any known metadata, and the method of storage. Depending on the particularity of the court, the witness may be required to testify regarding the chain of custody, including familiarity with the server structure and drive where the evidence was saved. However, many times this person is an attorney, paralegal, or law firm employee who may no longer be employed by the firm, or for a variety of strategic reasons, the person may not be an ideal or viable witness. In addition, attorneys must avoid the possibility that they become a witness to authenticate their own evidence obtained online. Instead, attorneys are better served to have the plaintiff qualified as the "witness with knowledge." Relying on the plaintiff to authenticate evidence unfavorable to the plaintiff may not be ideal, however, and it would likely be the subject of a motion *in limine*. Hearsay considerations must also be considered if the evidence is a message or posting by a third party.

A forensic computer expert may be used to authenticate web evidence under 901(b)(3), which allows for authentication through "comparison with an authenticated specimen by an expert witness or trier of fact." The expert witness may be required to familiarize him- or herself with the metadata and the chain of custody of the tendered evidence. This method can be a costly and time-consuming and is typically used when the dispute is centered on the web evidence in question.

Rule 901(b)(4) instructs that authenticity may be established based on "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." Electronic evidence may be authenticated under Rule 901(b)(4) by producing the metadata of the collected web evidence, such as the URL, IP address, time- and date-stamps, user ID, and software and browser information. Although not conclusive, properly documented metadata is valuable evidence of authenticity under Rule 901(b)(4).

Rule 901(b)(9) provides another example of authentication as "[e]vidence describing a process or system and showing that it produces an accurate result." Producing evidence about the process or system used to collect web evidence may support a basis for admissibility. Such evidence may be in the form of an affidavit or witness testimony about how and when the online material was accessed, collected, and stored. A common example would be an IT professional familiar with the server structure and storage methods. In practice, this evidence would be provided in conjunction with the available metadata and Rule 901(b)(4).

Authentication with Assistance from Third Parties

Various companies have developed software aimed at resolving authentication issues. A handful of tech start-ups, including Page Vault, WebPreserver, and PageFreezer, have established themselves as early leaders in this niche, but burgeoning, industry. Most use a secure server that acts in conjunction with remote-browser architecture similar in appearance to a standard web browser, such as Internet Explorer, Firefox, or Google Chrome. Unlike the typical web browser, however, this software is specially designed to alleviate authentication concerns related to chain of custody and content alteration. Page Vault's software, for example, allows you to capture web evidence from your desk and save it to the company's remote server with only a few clicks of the mouse. A detailed metadata cover page is automatically generated and is included in the saved web capture. The metadata provided includes the time stamp, the website URL, the IP address, the browser, and the operating system. Then the web evidence remains saved in the permanent as-viewed format on Page Vault's remote server and may printed any time afterward in the exact format as it appeared at the time that the viewer captured the web evidence. The company will even provide an affidavit regarding its server structure and security upon request. Monthly packages for these services start at approximately $75 a month.

Presenting web evidence with the supporting metadata cover page in discovery or during a deposition can have a powerful effect on a witness and the opposing counsel, and it may quell the opposing counsel's thought of challenging the evidence at trial.

Updated Investigative Methods

Thanks to technology, attorneys today have several ways to collect evidence during investigations that our predecessors

did not, ranging from geotracking applications in "smart" devices to electronic subscription services, which conveniently collect data. Otherwise you can rely on "your fingertips."

Geotracking

Location tracking has become one of the defining features of "smart" devices. The two leading smartphones, iPhone and Android, both have location tracking enabled by default. For fitness bracelets and other "wearable tech," location tracking is not only a defining feature; it is practically their *raison d'etre*. And, as more and more home appliances join the ranks of devices that can connect to the internet—the "internet of things"—the practice of collecting location-based data will only become more commonplace. For privacy advocates, this is the stuff of nightmares. For defense lawyers, location tracking can be an extremely useful tool, especially when tracking social media activity.

Location-based social media monitoring, as the name implies, tracks social media activity within a defined geographical area using a virtual perimeter, or a "geofence." With a geofence, you can collect any tweet, Facebook post, or other social media activity that is geo-located within a defined geographical area. Several companies offer location-based social media monitoring services to meet the needs of businesses in a variety of fields, including law enforcement (DigitalStakeout, http://www.DigitalStakeout.com), retail and hospitality services (Local Measure, http://www.localmeasure.com), and litigation (X1, http://www.x1.com).

Upon receiving news reports of an accident (perhaps through the use of keyword-based alerts, discussed below), placing a geofence around an accident scene will gather and record all social media posts geo-located in the surrounding area, such as accident scene photographs taken by passersby. This is important, and quickly fleeting, evidence. Accordingly, the closer in time to the accident's occurrence, the more likely the geofence is to capture relevant data.

A geofence can also be a useful tool for trial. By setting up a geofence around a courthouse, the user will be able to track all public tweets and social media posts by jurors, witnesses, opposing counsel, and anyone else within the vicinity. This can be useful for all phases of trial, from voir dire to jury deliberations, and beyond.

Subscription Services

Subscription services, such as Lexis and Westlaw, both offer a range of services that can assist in gathering an array of background information about a person. Lexis Advance's Social Media Locator and WestlawNext's Web Analytics are both geared toward social media and web activity. For a broader swath of background information, try Lexis Advance Smart-Linx Comprehensive Person Reports and WestlawNext's PeopleMap Reports. Both reports include available information about the subject across a broad spectrum of categories, including basic background information (such as aliases, current and former addresses, e-mail addresses, Social Security numbers, and telephone numbers); asset information (tax records, property records, vehicle registrations, aircraft, and watercraft registrations); and adverse information (arrest and criminal records, lawsuits, bankruptcy filings, and judgments, among others).

Free Information at Your Fingertips

Another option that is more powerful, more comprehensive, and free: Google, the largest search engine in the world. Google processes over 70 percent of all internet searches conducted on desktop computers, and in 2015 it was handling more than 100,000 billion searches per month. *See* Desktop Search Engine Market Share, https://www.netmarketshare.com (last visited Oct. 18, 2016). *See also* Douglas McMillan, *Mobile Search Tops at Google*, Law Blog (Oct. 8, 2015), http://www.wsj.com (requiring subscription).

As with any powerful weapon, wielding it effectively requires some skill. Similar to the paid subscription services, Google has its own set of terms and connectors that can help a user harness the full power of Google. Useful tips when using Google's search terms and connectors include the following:

- When searching for an exact phrase, place the phrase within quotation marks and Google will only provide results that contain that phrase.
- To search for terms that appear within a certain number of words on a given web page, use *AROUND(x)* between search terms, with *x* representing the range of words. Note that *AROUND* must be in ALL CAPS for this tool to work properly. This tool helps eliminate false-positive results.
- Placing *filetype:* before the search term (with no intervening spaces) returns only search results of the specified filetype, with *x* representing the filetype sought. (Example: *"John Doe" filetype:PDF.*)
- By placing *OR* (in all caps) between search terms, Google will return search results that contain either phrase. (Example: *"John Doe" OR "Doe, John Q."* will return pages in which either phrase appears.) This eliminates the need to conduct multiple searches using multiple permutations of the search terms.
- Placing two periods between two dates (again, with no spaces) will return results from within the designated time range. (Example: *DRI 2005..2010* will return only results from within the specified date range.) This also works with prices (*e.g.*, *iPhone $50..$100*) or any range of numbers.
- To search for pages that do not include a specific term, place the minus sign or the word *NOT* (in all caps) before the excluded term. (Examples: *viper –animal*; *viper NOT animal*.)
- To search for terms appearing in the title, use *intitle:* followed (with no space) by the search term.
- To limit the scope of the search to a specific webpage, add *site:* to the end of your search query followed (with no space) by the URL of the website to be searched. This is particularly useful for poorly designed websites. (Think: rural local news website.) If the search on the website is not returning an archived news story that you know exists, this can help find it.
- A similar feature is the link-specific search. Use *link:[URL]* to search for pages that link to a certain site. (Example: *link: www.smurfsightings.com* will return only webpages that link to the listed site.)
- To find sites that are related to a specific site, use *related:[URL].* (Example: *related:arcticsharkfishing.com*.)

- Use a tilde (~) immediately before a search term (with no space) to include results containing the term or its synonyms.
- To get results containing terms often used in association with your search term, use an asterisk before the term (with no space).
- For scholarly papers written by a particular author, use *author:* followed (with no space) by the name of the author that you want to read.
- In addition to searching for the subject's name, it is suggested to search the subject's email address or addresses as well. This is particularly useful when searching plaintiffs with common names when it is nearly impossible to successfully search for and locate a specific "John Smith."

As with any powerful weapon, wielding it effectively requires some skill. Similar to the paid subscription services, Google has its own set of terms and connectors that can help a user harness the full power of Google.

Keyword-based monitoring allows tracking of content from specified internet sources based on specified keywords. A number of companies offer this service. Google, for example, has a free service called Google Alerts that will automatically update the user when a specified keyword is published on the internet. Similar services include Addictomatic (http://www.addictomatic.com), Twazzup (http://www.twazzup.com), Social Mention (http://www.socialmention.com), and X1 Social Discovery (http://www.x1.com). The potential uses for keyword-based monitoring are vast. For example, a lawyer might use keyword-based monitoring to receive an e-mail whenever a news story is published regarding a collision occurring in the lawyer's state involving a vehicle manufactured by his or her client. Lastly, searching http://www.youtube.com with your plaintiff's e-mail address may uncover valuable and interesting evidence to support your case.

Technological Ignorance Is No Longer an Option

Before engaging in advanced investigative techniques, you must understand the ground rules. In 2012, the American Bar Association (ABA) modified the comments to the Model Rules of Professional Conduct to address technological competency, stating that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*." Model Rules of Prof'l Conduct R. 1.1, amended cmt. 8 (2012).The ABA comments call for attorneys not only to understand technologies, but also to understand the "benefits and risks of relevant technology." This means that attorneys must understand the types of evidence that new technologies can help uncover, how to access such evidence, how that evidence can be used, and the relevant admissibility considerations associated with each form of evidence. Some states have created similar obligations. *See, e.g.*, *State v. Ratliff*, 2014 ND 156, 849 N.W.2d 183 (N.D. 2014) (ruling that attorneys have an ethical duty to be competent in regard to technological issues related to evidence and stating that lawyers and judges alike must be increasingly vigilant to this end); *James v. Nat'l Fin., LLC*, C.A. No. 8931-VCL, WL 2014 6845560, at *12 (Del. Ch. Dec. 5, 2015) (granting plaintiff's motion for sanctions and stating that "[p]rofessed technological incompetence is not an excuse for discovery misconduct" in response to an attorney telling the court that he was computer illiterate). As the trend continues to favor admissibility of digital evidence, court sympathy for technological ignorance will likely wane. This will give rise to risks for lawyers who fail to stay current with legal technology.

The ABA Model Rules apply in cyberspace. An overly aggressive social media campaign could easily run afoul of many Model Rules, such as Rule 4.1 (Truthfulness in Statements to Others); Rule 4.2 (Communication with Person Represented by Counsel); Rule 4.3 (Dealing with Unrepresented Person), Rule 5.3 (Responsibilities Regarding Non-Lawyer); and Rule 8.4 (Misconduct).

In one state-based example, the Philadelphia Bar Association expressed the view that a third party is not permitted to "friend" a witness under the Pennsylvania Rules of Professional Conduct to gain access to private information without revealing the true nature of the request and the association with the attorney. Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-2 (2009). In a similar case, demonstrating how courts are also defining the rules of engagement for attorneys conducing social media discovery searches, the New Jersey High Court held that regulators may pursue a case against attorneys accused of using a paralegal to "friend" a litigant to gain access to the litigant's non-public Facebook pages. Jacob Gershman, *Lawyers Accused of Facebook Spying Can Face Ethics Complaint, State High Court Rules*, Law Blog (Apr. 19, 2016), http://www.wsj.com (requiring subscription). In Ohio, an assistant district attorney created a fictitious Facebook page to contact a witness. The attorney was fired and received one year of probation from the disciplinary board for violating Model Rule 8.4, which makes it a violation to engage (directly or indirectly) in misrepresentation. *Disciplinary Counsel v. Brockler*, 145 Ohio St. 3d 270, 48 N.E.3d 557 (Ohio 2016).

Plaintiffs also have a duty to preserve evidence, including online evidence. A New Jersey court found that a plaintiff who deactivated his Facebook account, rather than turning over the information as ordered by the court, could be deemed to have destroyed evidence, which could result in sanctions for spoliation. *Gatto v. United Airlines, Inc., et al.*, 2:10-cv-01090, 2013 WL 1285285 (D. N.J. Mar. 25, 2013).

In another example, a Virginia attorney was sanctioned $542,000 and faced a disciplinary hearing in which the lawyer agreed to a five-year suspension for instructing his paralegal to counsel a client to remove prejudicial Facebook photos.

Allied Concrete Co. v. Lester, 736 S.E.2d 699 (Va. 2013). Other tribunals have been more lenient. The Florida Bar Professional Ethics Committee stated that, provided that there is no violation of rules or law pertaining to the preservation or spoliation of evidence, a lawyer may recommend that a client remove information relevant to the foreseeable proceeding as long as an appropriate record of the social media information or media is preserved. Florida Bar Ass'n Prof'l Ethics Comm., Proposed Advisory Opinion 14-1 (2015) (non-binding).

Social media and advanced internet research applies to jurors as well. The ABA is currently examining the permissible social media interaction with jurors. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 466. The ABA opinion states that a lawyer cannot directly or indirectly send an access request to a juror's social media and that an access request is considered a communication that would be the type of ex-parte communication prohibited by Model Rule 3.5(b). The opinion further provides that a lawyer is not prohibited from reviewing a juror's or a potential juror's internet presence, but a lawyer may not communicate with a juror or a potential juror, either directly or through another person. *Id*.

Best Practices

Timing is everything. Searches should be conducted at the outset of a case and updated every few months. Creating a specified checklist of websites for your staff or investigator is also a good practice. Facebook, Instagram, YouTube, Tumblr, Vine, and Twitter should be included. Use a plaintiff's e-mail address in your searches for more accurate results.

More is better. If you choose to conduct the searches and save the material yourself, be sure to record the HTML and DOM source file, the IP address, the date, and the time and familiarize yourself with your server structure and storage methods. Include this information in an affidavit at the time that you locate and save the web evidence, but don't become a witness to authenticate your own evidence. Be prepared to cite the relevancy and authenticity basis under your applicable state or federal rules, including Federal Rule of Evidence 901.

Invest. Consider purchasing software from a third party to streamline the online capture methods. Reasonable monthly options are available from several providers.

Use discovery. Analyze case details to determine if a stipulation or requests to admit will help in the authenticity battle. Send discovery requests regarding e-mail addresses and social media accounts. Courts have struggled to determine what social media evidence should be subject to discovery requests, so narrowly tailor the parameters of your discovery. Serving a subpoena upon a social media site will not be successful under most circumstances due to the Stored Communications Act, 18 U.S.C sec. 2701–2712. The act prohibits social media sites from producing private information without consent of the user.

Be professional. Be mindful of the rules and duties of your jurisdiction, which includes having a familiarity with technology. Do not overstep your bounds when conducting an investigation online. FD