From FOIA to Social Media

Investigating Plaintiffs and Potential Jurors

By Shawn Shepard and David C. Marshall

Staying informed about changes to the laws affecting case investigations has many benefits; among others, it can save you and your client time and money and protect you from ethical violations.

A critical part of any investigation is to know where and how to get records related to your subjects. Whether searching for online public records, requesting records from a state archive, performing field research in a local civil court clerks' office, or capturing potentially damaging comments on a subject's social media profile, staying abreast of the latest legal developments governing records access and retrieval can save time and money, protect you from ethics violations, and ensure that the documents relevant to your case are admissible in court. This article explores recent changes in federal and state open records laws, as well the current law governing electronically stored information, specifically as it relates to social media sources.

Federal Freedom of Information Act and FOIA Improvement Act of 2016

The federal Freedom of Information Act (FOIA), enacted in 1966, underwent significant reforms just two years ago with the passage of the FOIA Improvement Act of 2016. The 2016 legislation codified a "presumption of openness," adopting the U.S. Department of Justice's policy that documents subject to the FOIA would not be withheld unless the disclosure would result in foreseeable harm. Specifically, the FOIA now provides that an agency may withhold information only if it "reasonably foresees that disclosure would harm an interest protected by" one of the FOIA exemptions or if "disclosure is prohibited by law." 5 U.S.C. §552(a)(8)(A)(i). Agencies must also "consider whether partial disclosure of information is possible" and "take reasonable steps necessary to segregate and release nonexempt information." *Id.* §552(a)(8)(A)(ii).

The FOIA Improvement Act of 2016 included several particularly significant provisions for investigators. First, it codified the "Rule of 3," requiring agencies to make records "available for public inspection in an electronic format" if those

■ Shawn Shepard is an assistant director and senior investigative report writer with Smith & Carson, an investigative research firm that performs complex fact investigations, social media investigations, and juror research and analytics. She is a licensed attorney and private detective in Georgia, focusing on prod-uct liability, personal injury, and wrongful death investigations. David C. Marshall is a partner in the firm of Hawkins Parnell & Young in Atlanta. He serves as national coordinating counsel and lead trial counsel for various product manufacturers, contractors, and premises owners. He is licensed in Georgia, Florida, Illinois, New York, Texas, Missouri, and West Virginia. Before entering private practice, he served as an assistant district attorney and has tried over a hundred cases to verdict.

records "have been requested 3 or more times." *Id.* §552(a)(2)(D)(ii)(II). It also limited the ability of the government to charge search and duplication fees, prohibiting the assessment of fees when the government has failed to comply with notice deadlines set forth in the FOIA. *Id.* §552(a)(4)(A)(viii). Finally, it paved the way for a new online system for document requests. The 2016 legislation mandated that the Office of Management and Budget, in consultation with the Attorney General, "ensure the operation of a consolidated online request portal that allows a member of the public to submit a request for records… to any agency from a single website." *Id.* §552(m)(1). This provision, however, was not meant to alter the power of any other agency to create or maintain an independent online portal for the submission of a request, but it did require the Office of Management and Budget to establish standards "for interoperability between the portal" and "other request processing software" used by the agencies. *Id.* §552(m)(2).

The new online portal, dubbed the National FOIA Portal, launched this past May at https://www.foia.gov. The website is touted as a government-wide portal "that allows the public to submit a Freedom of Information Act request to any agency from a single place," but in fact, the current iteration still requires a requester to access several different websites, depending on the agency or agencies at issue. Dep't of Justice, Office of Pub. Affairs, *Department of Justice Announces Launch of National FOIA Portal* (Mar. 8, 2018). All 118 agencies covered by the FOIA are now linked to the portal in some way. For some agencies, a request may be submitted directly through an online form found at FOIA.gov. For others, the site redirects to either the agency's own website or https://FOIAonline.gov, a previously existing multi-agency platform. Before the

launch of the National FOIA Portal, the latter site, FOIAonline.gov, already handled 17 percent of the total volume of requests processed by the federal government. FOIA Ombudsman blog, *Cheers for a National FOIA Portal* (Sept. 11, 2017).

Overall, as of July 2018, the Government Accountability Office (GAO) found that federal agencies have only made partial progress in meeting the requirements of the 2016 amendments and have not even met all the requirements of the 2007 Open Government Act. *GAO Finds Only Partial Compliance with FOIA Revisions*, FEDweek (July 6, 2018). The GAO examined requirements under both laws requiring agencies to update response letters, implement tracking systems, provide FOIA training, maintain online records, designate chief FOIA officers, and update and publish comprehensive regulations. *Id.*

Public records laws are constantly changing, to such an extent that even watchdog groups and open records advocates have trouble keeping up. Often the changes involve the inclusion of additional exemptions for the type of information that an agency can withhold in response to a records request.

Additional Reading:

Tara J. Lamer, *You Can FOIA a FOIA (Seriously) – And You Should Probably Care (Seriously)*, Smith & Carson.

State Public Records Laws

Public records laws are constantly changing, to such an extent that even watchdog groups and open records advocates have trouble keeping up. Often the changes involve the inclusion of additional exemptions for the type of information that an agency can withhold in response to a records request. But several states have recently undergone substantial revisions of their public records statutes, either in response to public events or to the changing technology of records delivery and storage. The following are a few notable revisions by the states in the past two years.

Colorado

In August 2017, Colorado "modernized" its Open Records Act, which was the first major update of the law since its enactment 20 years ago. *Seven Things to Know About How Colorado's Open Records Law is Changing*, Colo. Freedom of Info. Coal. (June 1, 2017). The revisions focused primarily on the technological aspects of document delivery. The act now requires that digital records be provided in digital format and that sortable and searchable digital records be made available to the public in a sortable or searchable way. Colo. Rev. Stat. §24-72-203(3.5)(b). Before this amendment, an agency could produce electronically stored information as paper copies, thereby preventing a recipient from accessing available metadata. Anthony Edwards, *Colorado Open Records Act Goes "Native"* (Sept. 9, 2017). The provision is subject to the technological or practical feasibility of providing documents in these formats, but an agency must make "reasonable inquiries" about feasibility before providing the record in an alternate format or denying the request. Colo. Rev. Stat. §24-72-203(3.5)(c).

Florida

Before July 2017, Florida was one of a handful of states that allowed the public to request workers' compensation claim records. With the enactment of section 440.1851 of the Florida Statutes, Florida created an exemption for the "personal identifying information" of an injured or deceased worker appearing in the records of the Florida Department of Financial Services. Because even the name of a worker is now considered confidential and exempt in Florida, the agency is no longer maintaining its searchable online database or releasing any claims records.

The expressed intent of the legislation is to protect information about workers of a "sensitive, personal nature," but the bill also acknowledges that the release of the information was resulting in the "unwanted solicitation of injured workers and their families." H.B. 1107 §2 (Fla. 2017). Interestingly, the Florida Department of Financial Services reported in its agency analysis of the bill that it received approximately 90 requests per month for the names and contact information for injured or deceased workers that were reported to the department in the previous month, and most of those requests were from law firms. H.R., *Final Bill Analysis of H.B. 1007* (Fla. June 28, 2017) (citing Fla. Dep't Fin. Servs., *Agency Analysis of 2017 HB 1107*, at 1, (Mar. 8, 2017)). Each month, the resulting list included an average of 4,750 names, which were then provided to the requesters. *Id.* At least one commentator lauded the bill for "ensur[ing] that when workers are injured on the job… they will not be bombarded by phone calls and direct-mail pieces promising that they'll get rich off the injuries." Carol Bowen, *Commentary: Florida in Workers' Compensation Purgatory: Which Way Out?* Orlando Sentinel (June 1, 2017).

Although this new exemption to the public records law eliminated a useful tool for obtaining workers' compensation records in Florida, the exemption may not be around forever. The provision is subject to the Open Government Sunset Review Act and will be automatically repealed on October 2, 2022, if not re-enacted by the legislature. Fla. Stat. §440.1851(3).

Additional Reading:

Shawn Shepard, *The Confidentiality of Florida Workers' Compensation Records After HB 1107*, Smith & Carson.

Massachusetts

The Act to Improve Public Records, which became effective January 1, 2017, passed "sweeping changes" to the Massachusetts public records law and was the biggest overhaul to the public records law in 40 years. *Massachusetts Law About Freedom of Information and Public Records*, Commonwealth of Mass. (compilation by the Trial Court Law Libraries) (last updated June

18,2018). Massachusetts' public records law had previously been considered one of the weakest public records laws in the country because there was "no real penalty for noncompliance." Joshua Miller, *State Panel Advances Public Records Bill*, Boston Globe (July 16, 2015).

The Massachusetts public records law now requires agencies to provide public records to a requester in electronic format unless the record is not available in an electronic format or the requester does not have the ability to receive or access the record electronically. Mass. Gen. Laws ch. 66 §6A(d). Similar to the federal FOIA, Massachusetts agencies are now required to provide electronic copies of commonly requested records on a searchable website. *Id.* ch. 66 §19(b). Agencies are also required to permit inspection or provide a copy of a requested record within 10 business days following receipt of the request, but they may petition the supervisor of records for an extension if needed. *Id.* ch. 66 §10(a) & (c). Other notable provisions include limiting fees for employee search time and providing for an award of attorney's fees and costs in court actions against an agency when a requester prevails. *Id.* ch. 66 §§10(d), 10A(d)(2).

Oregon

Oregon passed four bills related to public records in July 2017. The bills were the most significant revisions in 44 years and were reportedly in response to frustrations in the state about the difficulty of obtaining documents related to the administration of the prior governor who ultimately resigned. Diane Dietz, *What to Know About Oregon's Four New Public Records Laws*, Statesman J. (July 11, 2017). Effective at the beginning of 2018, a public agency in Oregon now has five business days either to acknowledge or complete a records request. Or. Rev. Stat. §192.324(2) (2017). After acknowledging a request, the agency has 10 additional business days either to complete the request or provide a statement that the request is still being processed along with a reasonable estimated completion date. *Id.* §192.329(5). Completing the request means either providing access or copies of nonexempt records; asserting exemptions; separating exempt from nonexempt material and making the nonexempt material available; providing a statement that the agency is not the record custodian; or providing a statement that the agency is prohibited by law from acknowledging that a record exists. *Id.* §192.329(2)(a-e).

Other changes included establishing the Oregon Sunshine Committee to review the 550-plus exemptions that had been created during the law's 44-year existence, creating a public records advocate to help resolve disputes, and appointing a chief data officer to make the state's online databases more accessible to the public. *Id.* §§192.511, 192.461, 276A.353.

South Carolina

Effective May 2017, South Carolina adopted several changes to its Freedom of Information Act. The new legislation expressly provided that individuals have the right to request and receive public records by electronic transmission but that an agency is not required to provide an electronic version if one does not already exist. S.C. Code Ann. §30-4-30(A)(1), (2). The South Carolina legislation also limited fees, reduced response times, and added a deadline for document production. S.C. Code Ann. §30-4-30(B), (C). Section 30-4-30(A) provides that an agency cannot charge a copy fee if records are in electronic format and are transmitted electronically, but the agency can charge for staff time required to transfer documents to that format. It also provides that an agency can require a fee deposit but that the deposit cannot exceed 25 percent of the reasonably anticipated costs for reproduction of the records. With respect to timing, an agency now has 10 days to provide a response about the availability of a record if a record is less than two years old and 20 days to respond if the record is older. The agency then has 30 or 35 calendar days to produce the records, depending on the document age. S.C. Code Ann. §30-4-30(C).

Social Media

With approximately 69 percent of Americans using at least one social media platform today, researching a subject's social media accounts, whether the subject is a litigant, witness, or potential juror in a case, has become an essential investigative tool. Not surprisingly, age is a factor in social media use, but statistics show that the need to complete social media research about subjects is not limited to younger people.

According to the Pew Research Center, Facebook continues to dominate the social media industry, with approximately two-thirds of all Americans using the platform. Aaron Smith and Monica Anderson, *Social Media Use in 2018*, Pew Research Ctr. (Mar. 1, 2018). While younger users reported the highest use—with 81 percent of 18 to 29-year-olds and 78 percent of 30 to 49-year-olds having a profile in 2018—as many as 65 percent of people ages 50 to 64 and 41 percent of people over 65 also use the site. *Id.* Older users are also well represented on other social media platforms. Of respondents ages 18 to 29, 64 percent reported use of Instagram while 40 percent reported use of Twitter, compared with 21 percent and 19 percent of respondents aged 50 to 64, respectively, using the same websites. *Id.*

Massachusetts' public records law had previously been considered one of the weakest public records laws in the country because there was "no real penalty for noncompliance."

Given the widespread use of these platforms, the chances are good that the subjects in your case will have one or more social media accounts. But when locating, obtaining, and capturing these social media profiles, an attorney must consider the ethical obligations for both the attorney and the attorney's employees and contractors, as well as the law affecting the potential use of the profiles during litigation.

Ethical Considerations

In most jurisdictions, having familiarity with current technology is part of the duty of competence of an attorney. Rule 1.1 of the ABA Model Rules of Professional

Conduct states that a lawyer must provide "competent representation to a client," which requires "the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." Comment 8 to Model Rule 1.1 explains that to maintain the requisite skill and knowledge, a lawyer "should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." At least 34 states have adopted comment 8 as of this writing, with the most recent addition being Vermont. Bob Ambrogi, Two More States Have Adopted Duty of Tech Competence; Total Now 34, LawSites (Dec. 7, 2018).

As for the ethics of researching social media profiles, the general consensus is that an attorney is permitted to access the public portion of a party or nonparty's social media profile. But neither an attorney nor the attorney's agents can use deception or trickery to gain access to the non-public portion of a social media account.

State and local ethics opinions have addressed what this duty of competency in technology means when it involves social media. According to the District of Columbia Bar, "[t]he guiding principle for lawyers with regard to the use of any social network site is that they must be conversant in how the site works. Lawyers must understand the functionality of the social networking site, including its privacy policies." D.C. B. Legal Ethics Comm., Ethics Op. 370 (2016). The Pennsylvania Bar Association has stated more generally that "a lawyer should (1) have a basic knowledge of how social media websites work, and (2) advise clients about the issues that may arise as a result of their use of these websites," while the New Hampshire Bar has explained that the duty specifically includes being "aware of social media as a source of potentially useful information in litigation," being "competent to obtain that information directly or through an agent," and knowing "how to make effective use of that information in litigation." Penn. B. Ass'n, Formal Op. 2014-300 (2014); N.H. B. Ass'n, Advisory Op. 2012-13/05 (2012). The New York State Bar Association has acknowledged that "[a]lthough a lawyer may not delegate his or her obligation to be competent, he or she may rely, as appropriate on other lawyers or professionals in the field of electronic discovery and social media in obtaining such competence." N.Y. St. B. Ass'n, Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York State Bar Association (May 11, 2017).

As for the ethics of researching social media profiles, the general consensus is that an attorney is permitted to access the public portion of a party or nonparty's social media profile. But neither an attorney nor the attorney's agents can use deception or trickery to gain access to the non-public portion of a social media account. In other words, an attorney cannot pose as someone else to friend a person and gain access to their information, nor can the attorney use a third party, such as a paralegal or an investigator, to make that request. Rules 4.1(a) and 8.4 of the Model Rules of Professional Conduct prohibit an attorney from making a "false statement of material fact or law to a third person" and from engaging "in conduct involving, dishonesty, fraud, deceit or misrepresentation." Model Rule 5.3(b) requires a lawyer "having direct supervisory authority" over a nonlawyer to make "reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer." An attorney is also prohibited from knowingly assisting or inducing another to violate the Model Rules of Professional Conduct or to violate the rules though the "acts of another." Model Rules of Prof'l Conduct R. 8.4.

Sending a friend request is not prohibited in all circumstances, though. A New York ethics opinion notes that an attorney can send a request to an unrepresented person to get information from the account for the purposes of litigation, without disclosing the reason for the request, as long as the attorney uses his or her real name and profile. N.Y. St. B. Ass'n, Ethics Op. 2010-2 (Sept. 2010). Other state and local bar associations require additional disclosures, mandating not only the real name and profile of the attorney but also the attorney's affiliation and purpose. N.Y. St. B. Ass'n, Social Media Ethics Guidelines, *supra* (citing rules of the bar associations of New Hampshire, Massachusetts, San Diego, and Philadelphia).

An attorney must take even more care when researching the social media profiles of a represented person due to Model Rule 4.2, which prohibits communication with a represented person without consent of the other lawyer or as authorized by law. While it goes without saying that an attorney cannot send a friend or connection request to a represented person, New York has noted that even an automatic notification that an attorney has viewed a social media profile can constitute a communication in violation of Rule 4.2. *See* N.Y. St. B. Ass'n, Social Media Ethics Guidelines, *supra* (acknowledging that the New York ethics opinions on the topic pertained to communications with jurors but drawing a comparison to persons represented by counsel). This position differs with that of the American Bar Association and jurisdictions such as Colorado, District of Columbia, and Pennsylvania. Rob Cary, *Jury Selection 2.0: Ethical Use of the Internet to Research Jurors and Potential Jurors*, 33 Law Man. Prof. Conduct 721 (Dec. 13, 2017).

An example of an automatic notification includes that of LinkedIn, which alerts an account holder that a person has viewed his or her profile. Instagram also briefly had a similar notification, starting in February 2018, when it tested a feature through which users were notified when someone took a screenshot of their story. Within four months, Instagram had ceased the test. Lulu Chang, *Creep in Peace – Instagram Will No Longer Tell People When You*

Take Screenshots, Digital Trends (June 15, 2018). Another area of potential concern that has not been widely addressed by the courts or in ethics opinions is notification through IP address capture that an attorney has viewed a person's personal website or blog. *See generally* Rafael Olmeda, *Judge's 'Pathetic, Miserable' Life Threatened, and It Came From a Former Judge's Account*, Sun-Sentinel (Aug. 22, 2018) (discussing how an IP address from a threatening blog comment was traced to a former county court judge).

With respect to jury research, an attorney is generally permitted to review the public social media presence of jurors and prospective jurors, but whether the attorney is *required* to conduct online juror research as part of the attorney's duty of competence depends on the jurisdiction. The caveats to juror research include prohibitions on such research imposed by a particular judge or court and the limitation on ex parte communications with jurors, which may be triggered by automatic notification, discussed above. Cary, *supra*.

As for an affirmative duty, the Missouri Supreme Court has found that attorneys have a duty to perform online research about a prospective juror's litigation history and "bring reasonable suspicion of juror nondisclosure to the trial court's attention prior to jury empanelment." *Johnson v. McCullough*, 306 S.W. 3d 551 (Mo. 2010). The court did not address social media profiles, but the opinion did discuss an online court system that provided access to the civil history of venire members. *Id.; see also King v. Sorenson,* 532 S.W. 3d 209 (Mo. App. Ct. 2017) (recognizing the "narrow parameters" of the court rule adopted in response to the case, which expressly requires background Internet searches on potential jurors to Case.net searches of a potential juror's litigation history). Other courts have adopted standing orders that expressly allow online juror research without affirmatively requiring it. *See* Ben Hancock, *Should You 'Facebook' the Jury? Yes. No. Probably.*, Law.com (April 26, 2017).

Finally, as defense counsel, you should be aware of potential spoliation issues that can arise with social media evidence. Capturing public social media early through informal discovery can help to determine whether spoliation issues have occurred. Ethics violations involving the alteration of social media content have resulted in grave consequences for attorneys and their clients. *See Allied Concrete Co. v. Lester*, 736 S.E. 2d 699 (Va. 2013) (lower court assessed sanctions totaling $722,000 against an attorney and his client because the attorney told the client to "clean up" his profile and the client deleted 16 photos); Debra Cassens Weiss, *Lawyer Agrees to Five-Year Suspension for Advising Client to Clean Up His Facebook Photos*, ABA J. (Aug. 7, 2013).

An early social media capture can also be beneficial to the defense, given that attorneys are generally permitted to caution their clients against creating any new social media evidence during the pendency of an action and to advise clients about changing privacy and security settings either before or during litigation. *See* N.Y. St. B. Ass'n, Social Media Ethics Guidelines, *supra*.

Additional Reading:

Andrea Jewett, *Before You Accept That Friend Request or Publish That Post: Ethical Issues in Consideration for Social Media Interaction*, 24 Ga. B.J. 19 (Aug. 2018).

Authentication

If social media evidence relevant to your case has been captured during an investigation, you want to know that you can use that content in court. In most cases, litigants will stipulate to the authenticity of social media evidence, but when the evidence is particularly damaging, the proferring party may be in for a fight. Recent changes to the Federal Rules of Evidence that are designed to streamline this process specifically address the self-authentication of electronically stored information, which includes social media profiles. While time will tell how helpful these provisions are for social media evidence, the adoption of the provisions takes nothing away from existing methods of authentication.

The amendments to Rule 902 of the Federal Rules of Evidence, which added subsections (13) and (14), went into effect on December 1, 2017. Self-authenticating evidence under Rule 902 now includes "[a] record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of 902(11) or (12)." It also includes "[d]ata copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of 902(11) or (12)." Fed. R. Evid. 902(14). The latter, Federal Rule of Evidence 902(14), pertains to user-created data and is the section that applies to social media evidence.

As defense counsel, you should be aware of potential spoliation issues that can arise with social media evidence. Capturing public social media early through informal discovery can help to determine whether spoliation issues have occurred. Ethics violations involving the alteration of social media content have resulted in grave consequences for attorneys and their clients.

Federal Rule of Evidence 902 does not define a "qualified person," but the advisory committee's notes to the rule state that a proponent of the evidence "must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial." The notes also state that data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value," a sequence

of numbers or characters produced by an algorithm based on the digital contents of a drive, medium, or file. Identical hash values for a copy and an original "reliably attest to the fact that they are duplicates," and self-authentication is proper when a qualified person certifies that he or she has checked the hash value of the proferred item against the hash value of the original and the two are the same. Fed. R. Evid. 902 advisory committee's notes.

Because other grounds will likely be necessary to authenticate social media evidence given its nature, taking care when capturing it is important.

Although a hash value can be given to a social media profile at the time of capture that can be compared to the hash value of the profile offered at the time of the trial, that hash value may not address all questions of authenticity for the evidence. For example, the authenticity of social media evidence has been challenged when a party has claimed that the account could not be attributed to that party or that the purported owner of the account did not make the posts in question. *See, e.g., Griffin v. State*, 19 A.3d 415 (Md. 2011); *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012). In these circumstances, the social media evidence likely cannot be authenticated through a process of digital identification alone and other foundational evidence will need to be provided. The new amendments in fact require a proponent to provide written notice in advance of its intent to offer the record and to make the record and the certification available for inspection so that the other party has an opportunity to challenge it. Fed. R. Evid. 902(14) (referring to the notice requirements of Rule 902(11)). Further, the advisory committee's notes acknowledge that even if a certification sufficiently establishes that a webpage is authentic, a "[a party] remains free to object that the statement on the webpage was not placed there by [the party]."

The amendments raise a question about whether social media evidence can be self-authenticated under Federal Rule of Evidence 902(14) through any other method than hash values. The advisory committee's notes indicate that the rule is meant to be "flexible enough" to allow certifications through other processes. Arguably then, could it be enough to offer a certification from a qualified person attesting to, among other things, the digital methods used to capture the profile, the validity of descriptive metadata on the profile, and the integrity of the content from the date of capture? *See* Fed. R. Evid. 902 advisory committee's notes. It is currently unclear whether this evidence would be adequate to show a "process of digital identification" as required by the subsection.

But even if social media evidence cannot be self-authenticated under Federal Rule of Evidence 902(14), Rule 901 continues to provide a variety of grounds by which it can be admitted. Federal Rules of Evidence 902(13) and (14) were meant to simplify the introduction of electronic evidence, and the advisory committee's notes recognize that "[n]othing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate." Notably, Rule 901 provides a nonexhaustive list of evidence that can be used to support a finding that the item is what the proponent claims, including the testimony of a witness with knowledge, evidence of distinctive characteristics, and evidence about a process or system. Fed. R. Evid. 901(b)(1), (4), & (9). *See Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 541 (D. Md. 2007). *See also* Craig Ball, *Handy Chart on E-Admissibility*, Ball in Your Court blog (Apr. 2018) (commenting on and posting Paul W. Grimm & Kevin F. Brady, *Admissibility of Electronic Evidence* (2018)). Ultimately, one of the easiest ways to authenticate social media content remains having a party admit ownership and control of the content during discovery, again illustrating the importance of obtaining social media evidence at the beginning of a case.

Because other grounds will likely be necessary to authenticate social media evidence given its nature, taking care when capturing it is important. See Lorraine, 241 F.R.D. at 542 ("A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be… Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the ability to get evidence admitted because of a failure to authenticate it is almost always a self-inflicted injury which can be avoided by thoughtful advance preparation."). Best practices for social media evidence include capturing all the headers and footers when you make a copy to show the metadata, such as the full website address, the date, and the time; expanding all posts and preserving all sections and pictures in a profile; capturing the profile or post in a way that preserves the integrity of how the profile or post appears digitally; and performing sufficient research about a subject's online presence to corroborate the ownership of the account or authorship of the post. See Your ABA, How to Get Social Media Evidence Admitted to Court (June 27, 2017).

Additional Reading:

Sandra L. Ward, *The Rise of Social Media Evidence and the Necessity of Thorough Social Media Investigations*, Smith & Carson.

Conclusion

Staying informed about changes to the laws affecting case investigations, including the release of public records and the capture and use of social media evidence, can save you and your client time and money, help you avoid frustration in court, and protect you from ethical violations. For federal and state open records law, it is important to keep up with the current availability of records, the required times for responses, the type of delivery permitted, and any limitation on fees. For social media evidence, knowing what is permissible to do to acquire the content is essential for both you and your investigators, and complying with best practices for social media capture on the front end can ease getting the evidence admitted into court. FD