Social Media: What Every Litigator Needs to Know

NORMAN C. SIMON AND SAMANTHA V. ETTARI, KRAMER LEVIN NAFTALIS & FRANKEL LLP, WITH PRACTICAL LAW LITIGATION

Search the Resource ID numbers in blue on Westlaw for more.

This Practice Note discusses key issues about social media in various stages of litigation, including in the context of litigation holds, pre-litigation investigation, service of process, discovery, jury selection, and trial.

As technology progresses and sources of electronically stored information (ESI) proliferate, social media content is a part of the litigation equation that counsel and courts increasingly cannot ignore. From the pre-litigation stage through discovery and trial, social media content often is critical to a party's claim or defense. It can also pose significant challenges. Counsel must be aware of the potential impact of social media on all phases of litigation, as well as some ethical minefields concerning its use.

This Practice Note highlights key issues surrounding social media in litigation, including:

- The use of social media in the early stages of litigation.
- Special considerations for discovery and authentication of social media content.
- The role of social media in a jury trial.

For more resources to assist counsel and companies in identifying the legal risks of social media use, see Practical Law's Social Media Usage Toolkit. For a description of common categories of social media and a list of currently popular social media services, with non-legal, non-technical descriptions for each, see Practice Note, Social Media: A Quick Guide (0-501-1442). For resources on ESI generally, see E-Discovery Toolkit (8-503-1078).

EARLY STAGES OF LITIGATION

Even before a complaint has been drafted or filed, counsel should consider the potential applications of social media. In particular, social media may be a factor in:

- The parties' obligations to preserve and collect relevant evidence as part of a litigation hold (see Preservation; see also, for example, 2015 Advisory Committee Notes to Federal Rule of Civil Procedure (FRCP) 37(e) (noting the importance of counsel becoming familiar with clients' social media use to address preservation issues)).
- The pre-litigation investigation of potential adverse parties, witnesses, and opposing counsel (see Pre-Litigation Investigation).
- The parties' ability to locate and serve adverse parties (see Service of Process and Service of Other Documents).

PRESERVATION

The duty to preserve potentially relevant evidence arises when a party reasonably anticipates litigation, and may arise before an action is filed (see Practice Notes, Implementing a Litigation Hold: When to Implement a Litigation Hold (8-502-9481) and Reasonable Anticipation of Litigation Under FRCP 37(e): Triggers and Limits (W-008-2708)). This duty applies equally to social media content (see *Congregation Rabbinical Coll. of Tartikov, Inc. v. Vill. of Pomona*, 138 F.Supp.3d 352, 387-88 (S.D.N.Y. 2015); *Howell v. Buckeye Ranch, Inc.*, 2012 WL 5265170, at *2 (S.D. Ohio Oct. 1, 2012)).

In federal court, once litigation commences, the court's scheduling order may specifically provide for preservation of ESI, which could include social media content (FRCP 16(b)(3)(B)(iii)). The parties' discovery plan under the FRCP must include any issues regarding preservation of these materials (FRCP 26(f)(3)(C)).

Litigation Holds and Collection

As with other potentially relevant ESI, counsel should not overlook social media content in preservation or collection efforts (see *Caputi v. Topper Realty Corp.*, 2015 WL 893663, at *8 (E.D.N.Y. Feb. 25, 2015) (directing plaintiff to preserve all of her Facebook activity through the litigation's duration); *EEOC v. Original Honeybaked Ham Co. of Ga.*, 2012 WL 5430974, at *1 (D. Colo. Nov. 7, 2012) (likening certain social media content to an "Everything About Me" folder that is voluntarily shared with others); see also *Petion v. 1 Burr Rd. Operating Co. II, LLC*, 2017 WL 6453398, at *3 (D. Conn. Dec. 15, 2017); *Hawkins v. Coll. of Charleston*, 2013 WL 6050324, at *3 (D.S.C. Nov. 15, 2013)).

Counsel drafting a litigation hold should consider specifically referencing social media platforms, including any associated and

collectable metadata, among the potential sources of information that custodians should preserve. Similarly, counsel should consider identifying social media platforms as potential sources of relevant information in any demand letter sent to an adversary requesting preservation of relevant ESI.

Counsel may use printouts, screenshots, or web crawlers to capture, gather, and store static images of social media content. However, counsel should bear in mind that these formats may be inconsistent with the format sought in a request for production (document request) or subpoena, do not typically capture metadata, and may be insufficient for authentication (see Document Requests for Social Media Content and Authenticating Social Media).

Therefore, to collect social media content in preparation for a dispute, litigants should consider engaging an e-discovery vendor with appropriate expertise to harness the full range of content and metadata associated with the ESI. For resources on engaging an e-discovery vendor, see E-Discovery Toolkit (8-503-1078).

For more on key issues that companies and their counsel must consider to ensure compliance with their obligations to preserve and produce ESI, see Practice Notes, E-Discovery in the US: Overview (1-503-3009) and Practical Tips for Preserving ESI (8-500-3688). For more on document retention policies and implementing a litigation hold generally, see Litigation Hold Toolkit (2-545-9105). For a sample letter requesting that an opposing or third party preserve relevant evidence and information, see Standard Document, Document Preservation Letter (Demand) (6-535-8425).

Spoliation and Exposure to Sanctions

Digital realities increase the risk that a party or its counsel may be accused of spoliation by destroying or altering evidence. This is in part because not all clients appreciate the potential exposure to spoliation sanctions, given how easy it can be to delete, alter, or eliminate a digital file or social media post. Counsel should specifically instruct clients not to destroy or alter social media content where it may be relevant to an anticipated or ongoing litigation.

In federal court, absent an independent tort claim for spoliation under state law, FRCP 37(e) governs the imposition of sanctions or curative measures on a party who fails to take reasonable steps to preserve ESI that should have been preserved and over which the party has control (FRCP 37(e) and 2015 Advisory Committee Notes to FRCP 37(e)). If the lost ESI cannot be restored or replaced through additional discovery, the court may:

- Order measures no greater than necessary to cure any prejudice to another party from the loss of the ESI.
- Upon finding that the party who lost the ESI intended to deprive another party of the ESI's use in the litigation:
  - presume the lost information was unfavorable to the party;
  - instruct the jury that it may or must presume the information was unfavorable to the party; or
  - dismiss the action or enter a default judgment.

(FRCP 37(e)(1), (2). For more information on sanctions under FRCP 37(e), see Practice Note, Sanctions for ESI Spoliation Under FRCP 37(e): Overview (W-004-8150)).

Counsel therefore should not instruct or suggest to their clients that they intentionally alter, destroy, or disable social media content, because it puts both counsel and the client at risk for severe sanctions.

PRE-LITIGATION INVESTIGATION

The investigation of social media content can be highly effective to:

- Help develop a case.
- Frame potential causes of action.
- Resolve a dispute before reaching full-blown discovery.
- Create leverage for settlement.

When preparing a complaint or conducting due diligence in anticipation of litigation, counsel should, at a minimum, conduct internet and social media research on:

- The subject matter of the case.
- Potential parties.
- Opposing counsel.
- Potential witnesses.

However, before searching the social media content of a potential adversary or witness, counsel must understand:

- The applicable ethics rules for conducting pre-litigation investigation.
- How a user's privacy settings may impact the mechanics or ethics of pre-litigation investigation.

Ethical Considerations for Social Media Investigation

Many ethical guidelines and rules now require attorneys to learn and understand the basics of social media networks as part of their practice (see, for example, New York State Bar Ass'n (NYSBA) Social Media Ethics Guidelines (2017 NYSBA Guidelines), No. 1.A). These ethical guidelines and rules also often address how to handle social media content before and during litigation.

For example, many state and city bar ethical guidelines place limits on how counsel may access the social media content of opposing parties or witnesses for investigation purposes. These guidelines and opinions generally stem from the basic prohibition on directly or indirectly contacting a represented party without consent from that party's lawyer under the American Bar Association (ABA) Model Rules of Professional Conduct (ABA Model Rule 4.2).

A lawyer investigating a case generally:

- May access the public portions of a party's or witness's social media account, regardless of whether the party or witness is represented.
- May **not** access private or non-public portions of a **represented** party's or witness's social media account if the lawyer is required to "friend" or "follow" the account or account user.
- May "friend" or "follow" an unrepresented party or a witness on social media if the lawyer does not engage in deceptive behavior.

Using deception to "friend" or "follow" an unrepresented individual is uniformly deemed unethical, based on either or both:

- ABA Model Rule 4.1, which prohibits a lawyer from making a false statement of (or failing to disclose a) material fact to a third person.
- ABA Model Rule 8.4(c), which states that it is professional misconduct for a lawyer to engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.

However, the interpretation of deception differs across jurisdictions. In some jurisdictions, including New York, a lawyer can join a social network and connect with or "friend" an unrepresented individual without disclosing the reasons for the request if it does not involve any type of trickery. The lawyer cannot, for example, create a different or false name or profile to mask his identity (see, for example, 2017 NYSBA Guidelines, No. 4.B; New York City Bar Ass'n (NYCBA) Committee on Professional Ethics Formal Op. 2010-2, Obtaining Evidence from Social Networking Websites)). The lawyer must use her full name and an accurate profile.

Other states require a lawyer to affirmatively disclose her role in a dispute or litigation and identify the client and matter, reasoning that the failure to do so is an omission of a material fact and thereby amounts to deceptive conduct (see N.H. Bar Ass'n Ethics Committee Advisory Op. No. 2012-13/05 BA, Social Media Contact with Witnesses in the Course of Litigation; San Diego County Bar Ass'n Legal Ethics Op. 2011-2).

Some bar associations go further, requiring attorneys to inform the social media account holder of the intended use of the information, whether generally for litigation or specifically to impeach a witness (see Philadelphia Bar Ass'n Professional Guidance Committee, Op. 2009-02 (Mar. 2009), at 3)).

For more on ethical issues for lawyers in the context of social media generally, see Practice Note, Social Media Ethics for Attorneys (W-013-1896).

Privacy Settings

Privacy settings are crucial if a potential party or witness seeks to limit pre-discovery access to ESI. A user's privacy settings often dictate how much information a search may reveal. Therefore, counsel should try to protect a client's social media content from an adversary by maximizing the client's privacy settings. Conversely, an investigating lawyer should seek out as much relevant, public social media content as possible, in part because it can form the basis for requiring an adversary to disclose non-public information (see Relevance Considerations).

When advising a client to maximize privacy settings on any social media account, counsel should caution the client against deleting, altering, or disabling content on the account without also adequately preserving the content, or risk sanctions (see Spoliation and Exposure to Sanctions).

The investigating lawyer's own privacy settings are also important in certain circumstances. For example, some social media platforms, such as LinkedIn, do not allow a lawyer to surreptitiously view social media content without first selecting privacy options to make the lawyer anonymous. Without that setting adjustment, LinkedIn will notify the accountholder that his or her profile was viewed. In addition to alerting an adversary or witness to the lawyer's investigative efforts, these notifications may also be considered inappropriate and unethical contact when researching a potential jury pool or sitting juror, depending on the jurisdiction (see Researching Jurors on Social Media).

SERVICE OF PROCESS

Service is an area in which technological advances, including the proliferation of social media platforms, are reshaping procedural law. Over the past decade, many courts have embraced service of process via email, where due process is satisfied and the relevant state or international statutes or treaties allow for it (see, for example, *Advanced Access Content Sys. Licensing Adm'r, LLC v. Shen*, 2018 WL 4757939, at *6 (S.D.N.Y. Sept. 30, 2018); *Fraserside IP LLC v. Letyagin*, 280 F.R.D. 630, 631 (N.D. Iowa 2012); *U.S. Commodity Futures Trading Comm'n v. Rubio*, 2012 WL 3614360, at *3 (S.D. Fla. Aug. 21, 2012); but see *Joe Hand Promotions, Inc. v. Shepard*, 2013 WL 4058745, at *1-2 (E.D. Mo. Aug. 12, 2013)).

Some plaintiffs, when unable to perfect service through traditional means, have sought court approval to serve process using social media platforms such as Facebook and LinkedIn. Under this type of proposal, a plaintiff would send a message via the social media platform, attaching the summons and complaint, which the account holder could access upon logging into the site. Courts have denied these requests to serve process through social media sites for a number of reasons, including:

- Uncertainty surrounding the authenticity of social media accounts, given the potential for duplicate and false accounts (see, for example, *Fortunato v. Chase Bank USA, N.A.*, 2012 WL 2086950, at *2-3 (S.D.N.Y. June 7, 2012)).
- A lack of confidence that a message posted to a social media account is highly likely to reach defendants or satisfy due process requirements, particularly given users' ability to alter or dismantle their alert settings and notification methods (see, for example, *Miller v. Native Link Constr., L.L.C.*, 2016 WL 247008 (W.D. Pa. Jan. 21, 2016) (denying motion to serve process through LinkedIn); see also *FTC v. Pecon Software Ltd.*, 2013 WL 4016272, at *8 (S.D.N.Y. Aug. 7, 2013)).
- Where state law prohibits substitute service by electronic means on domestic defendants, and thus FRCP 4(e)(1) would prohibit service through Facebook in that state (see *Joe Hand Promotions*, 2013 WL 4058745, at *1-2).

However, some courts have allowed service of process via social media as an alternative method of service, particularly where defendants appear to have recently accessed and updated their social media accounts (see, for example, *Juicero, Inc. v. Itaste Co.*, 2017 WL 3996196, at *3 (N.D. Cal. June 5, 2017); *St. Francis Assisi v. Kuwait Finance House*, 2016 WL 5725002 (N.D. Cal. Sept. 30, 2016); *Ferrarese v. Shaw*, 164 F. Supp. 3d 361 (E.D.N.Y. 2016); *Lipenga v. Kambalame*, 2015 WL 9484473 (D. Md. Dec. 28, 2015); *WhosHere, Inc. v. Orun*, 2014 WL 670817 (E.D. Va. Feb. 20, 2014)).

In light of these cases, litigators seeking to serve via a social media platform should be prepared to:

- Prove the authenticity of related or associated email accounts.
- Demonstrate that the proposed service:
  - is not prohibited by applicable statutes or rules;
  - strictly complies with due process standards; and

- is highly likely to reach the defendant (for example, by showing that the defendant regularly views and maintains the social media account).

- Serve through email or another method in addition to social media.

SERVICE OF OTHER DOCUMENTS

Courts have allowed the service of motions and other post-summons documents through Facebook, where Facebook served as a secondary or "backstop" means of service, in addition to email (see, for example, *MetroPCS v. Devor*, 256 F. Supp. 3d 807, 808 (N.D. Ill. 2017)).

Courts have also permitted widespread notice of class action claims and settlements through social media, although typically counsel must accompany that with another form of notice (see, for example, *Allen v. Similasan Corp.*, 2017 WL 1346404, at *2 (S.D. Cal. Apr. 12, 2017); *In re Nat'l Collegiate Athletic Ass'n Student-Athlete Concussion Injury Litig.*, 314 F.R.D. 580, 603 (N.D. Ill. 2016); see also Practice Note, Settling Class Actions: Process and Procedure (3-541-8765)).

SOCIAL MEDIA IN DISCOVERY

Once litigation begins, counsel should ensure that discovery efforts cover social media content. Common issues that lawyers must address include:

- Determining whether the user (typically the adversary or a witness) or the social media provider is the right source of the desired ESI.
- Drafting appropriate document requests and interrogatories to reach relevant social media content through party discovery.
- Demonstrating the relevance and appropriate proportionality of discovery requests for social media content under FRCP 26(b)(1).
- Responding to discovery requests for social media content.
- Assessing how to authenticate social media content for use in summary judgment motions or at trial.

SUBPOENAS TO NON-PARTY SOCIAL MEDIA PROVIDERS

Securing social media content directly from a provider can be difficult. Some social media providers indicate on their websites or in other official documents that they may produce only limited user or account data or public content, but not private content, pursuant to a valid federal or state subpoena. These restrictions are driven in part by providers' concerns of running afoul of the Stored Communications Act (SCA), which prevents providers of electronic communication services from divulging private communications, and creates a set of statutory "Fourth Amendment-like privacy protections" (18 U.S.C. §§ 2701-2712; *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 971-72 (C.D. Cal. 2010)).

The SCA has been interpreted to cover certain private social media content, such as private messages and non-public posts or comments (see *Sines v. Kessler*, 2018 WL 3730434, at *2, *10 (N.D. Cal. Aug. 6, 2018) (quashing the portion of a subpoena seeking communications from a private, invite-only social networking and instant messaging platform because disclosure from the provider would violate the SCA); see also *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 667-68 (D.N.J. 2013) (holding that the SCA protected non-public wall posts on Facebook); *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012) (quashing a subpoena to Facebook for records from a deceased individual's Facebook account)).

Despite SCA-based objections to third-party subpoenas that sought production of a party's social media content because of concerns about the SCA, social network providers have provided alternatives. For example, Facebook has suggested that parties download the contents of their own accounts as an alternative method for producing the information through a tool available on Facebook. (See *Gatto v. United Air Lines, Inc.*, 2013 WL 1285285, at *2 (D.N.J. Mar. 25, 2013); *In re White Tail Oilfield Servs., L.L.C.*, 2012 WL 4857777, at *2-3 (E.D. La. 2012).) Other social media platforms also enable users to download account contents in a similar manner. Some courts have directly ordered parties to use this type of download tool and provide a copy of the report to their opponents in response to document requests (see, for example, *Rhone v. Schneider Nat'l Carriers, Inc.*, 2016 WL 1594453, at *3 (E.D. Mo. Apr. 21, 2016)).

For resources on using and responding to subpoenas in federal court generally, see Document Requests and Subpoenas in Federal Court Toolkit (3-590-9706).

DOCUMENT REQUESTS FOR SOCIAL MEDIA CONTENT

Discovery of social media content may be more successful through party discovery. As a best practice, counsel should craft document requests to reach social media content and related metadata by:

- Specifying that the definitions of "document" and "ESI" include social media content. For example:
  - "The term 'document' includes all information published at any time on any site or mobile application, including but not limited to all social networking or social media sites such as Facebook, LinkedIn, Twitter, Instagram, YouTube, or other social media providers."
  - "The term 'ESI' includes all content from social media providers and profiles and all related metadata."
- Including a separate document request that specifically seeks social media content. For example, "All social media postings, comments, messages, or other content relating to the allegations in the Complaint, including but not limited to content from Facebook, LinkedIn, Twitter, Instagram, YouTube, or other social media providers."
- Specifying in the instructions that documents and ESI must be produced with all available metadata. For example, "Electronically stored information ('ESI'), including but not limited to social media content, must be produced and continue to be preserved in its original native format with all relevant metadata, including but not limited to any author, creation date and time, modified date and time, native file path, native file name, and file type."
- Dictating the desired method of production for social media content, whether in native format, paper printouts, or PDF or TIFF formats.

Some courts have required parties to provide log-in and password access to an agent of the court for a pre-production in camera inspection of social media content (see, for example, *Original Honeybaked Ham Co.*, 2012 WL 5430974, at *3; *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371, at *1 (M.D. Pa. June 22, 2011)). Other courts have relied on user authorizations requesting that the social media provider produce the information (see, for example, *Gatto*, 2013 WL 1285285, at *1).

For a collection of resources on obtaining electronic discovery generally, see E-Discovery Toolkit (8-503-1078) and Document Discovery Toolkit (7-529-3645).

INTERROGATORIES CONCERNING SOCIAL MEDIA

Some US district courts have local rules restricting the scope of interrogatory requests so that a party may be limited from requesting specific social media platform and account information early in discovery. These rules also may require a party to use document requests or depositions to uncover social media platform and account information, or obtain a court order, before serving interrogatories seeking this type of information (for example, S.D.N.Y. L. Civ. R. 33.3).

If those limitations are not present, however, counsel may use interrogatories to identify:

- Social media platforms or accounts that the responding party established, used, or maintained.
- Email accounts or addresses and networks that are related to or associated with the responding party's social media accounts.
- All names, usernames, or pseudonyms, commonly referred to as "handles," associated with the responding party's social media accounts (because social media sites typically do not require an account holder to use his legal name).

The sworn responses to these interrogatories may be particularly important if the opposing party does not produce social media content or ESI and a motion to compel is required to reach that information, as that may enable sanctions against the opposing party (FRCP 37(a); see also Practice Note, Sanctions in Federal Civil Litigation: Sanctions Relating to Motions to Compel Disclosure or Discovery (W-001-1365)).

For more on using and responding to interrogatories in federal court generally, see Interrogatories in Federal Court Toolkit (9-555-3345).

RELEVANCE CONSIDERATIONS

Once formal discovery begins, relevant social media content is fair game. However, courts are sensitive to fishing expeditions, particularly as to social media content, which can be voluminous, burdensome, and costly to gather, review, and produce. Counsel should carefully tailor discovery demands to defend against objections, such as those based on relevance and proportionality under FRCP 26(b)(1).

For example, courts routinely:

- Refuse to grant unfettered access to social media (see, for example, *Terrell v. Memphis Zoo, Inc.*, 2018 WL 3520139, at *4 (W.D. Tenn. July 20, 2018); *In re Cook Med., Inc., IVC Filters Mktg., Sales Practices & Prod. Liab. Litig.*, 2017 WL 4099209, at *5 (S.D. Ind. Sept. 15, 2017); *Ehrenberg v. State Farm Mut. Auto. Ins. Co.*, 2017 WL 3582487, at *2 (E.D. La. Aug. 18, 2017); *Gordon v. T.G.R. Logistics, Inc.*, 321 F.R.D. 401, 405 (D. Wyo. 2017); *Roberts v. Clark Cty. Sch. Dist.*, 312 F.R.D. 594, 608 (D. Nev. 2016); *Lewis v. Bellows Falls Congregation of Jehovah's Witnesses, Bellows Falls, Vermont, Inc.*, 2016 WL 589867, at *2 (D. Vt. Feb. 11, 2016)).
- Limit access to a sampling of a party's activity on social media over a defined time period (see, for example, *Dewidar v. Nat'l R.R. Passenger Corp.*, 2018 WL 280023, at *5 (S.D. Cal. Jan. 3, 2018); *T.C on Behalf of S.C. v. Metro. Gov't of Nashville & Davidson Cty., Tennessee*, 2018 WL 3348728, at *15 (M.D. Tenn. July 9, 2018); *Gordon*, 321 F.R.D. at 406).

Many courts carefully analyze the allegations and requested social media content to tailor the production to only content that is relevant and proportional to the needs of the case, particularly in response to motions to compel discovery. Courts have narrowed the scope of the proposed discovery by, for example:

- Requiring the party seeking social media content, which the user has limited from public view, to make a threshold showing that the requested information is relevant, which may be supported by the user's publicly available social media content (see, for example, *Doe v. Rutherford Cty., Tenn., Bd. of Educ.*, 2014 WL 4080159, at *3 (M.D. Tenn. Aug. 18, 2014) (ordering plaintiffs' counsel to review restricted, nonpublic portions of only one of the plaintiffs' social media accounts and produce relevant information because, based on publicly available social media content, the evidentiary threshold was satisfied only as to that plaintiff); *Keller v. Nat'l Farmers Union Prop. & Cas., Co.*, 2013 WL 27731, at *4-5 (D. Mont. Jan. 2, 2013) (denying a motion to compel absent a threshold showing of relevance, but granting a request for a list of all social networking sites to which the plaintiffs belonged); see also *Potts v. Dollar Tree Stores, Inc.* 2013 WL 1176504, at *3 (M.D. Tenn. Mar. 20, 2013)).
- Providing detailed guidance on what social media content is relevant to the case and must be produced (see, for example, *Ehrenberg*, 2017 WL 3582487, at *3; *Gordon*, 321 F.R.D. at 406), including:
  - instructions about the relevance of a party's verbal communications, third-party communications, and photographs and videos to be produced (see, for example, *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 436 (S.D. Ind. 2010)); and
  - protocols to resolve any disputes on relevance or production (see, for example, *Thompson v. Autoliv ASP, Inc.*, 2012 WL 2342928, at *4-5 (D. Nev. June 20, 2012)).
- Ordering an *in camera* inspection, sometimes in connection with the appointment of a forensic expert special master, to identify relevant social media content from the plaintiffs' accounts (see, for example, *Connolly v. Alderman*, 2018 WL 4462368, at *6 (D. Vt. Sept. 18, 2018); *Original Honeybaked Ham Co.*, 2012 WL 5430974, at *2-3; *Offenback*, 2011 WL 2491371, at *1-2).
- Ordering a party's counsel, and not the party, to review the social media content and determine the relevance of the postings (see, for example, *Hinostroza v. Denny's Inc.*, 2018 WL 3212014, at *6-7 (D. Nev. June 29, 2018); *Lewis*, 2016 WL 589867, at *3; *Giacchetto*, 293 F.R.D. at 116-17; *Simply Storage*, 270 F.R.D. at 436; *Rutherford Cty. Tenn. Bd. of Educ.*, 2014 WL 4080159, at *3).
- Instructing the requesting party's counsel to review all social media content and inform opposing counsel of relevant information that was not produced, where the existing discovery record suggests that the producing party may have withheld information relevant to the litigation (see, for example, *Thompson*, 2012 WL 2342928, at *5).

PRIVACY CONSIDERATIONS

In addition to common objections like relevance or undue burden, parties facing discovery requests for social media content often have

invoked privacy as a reason to resist disclosure. However, courts generally are dismissive of privacy claims over the public content of social media accounts. The same is usually true for non-public social media content, even where a user has set his privacy settings to shield certain information. Because non-public content is available to select third parties, who may do with it what they wish, courts often reject privacy claims over relevant information. (See *Lewis*, 2016 WL 589867, at *2; *Chaney v. Fayette Cty. Pub. Sch. Dist.*, 977 F. Supp. 2d 1308, 1315-16 (N.D. Ga. 2013); see also *Hinostroza,* 2018 WL 3212014, at *6; *In re Cook Med.*, 2017 WL 4099209, at *5; *United States v. Meregildo*, 883 F. Supp. 2d 523, 525-26 (S.D.N.Y. 2012).)

Moreover, where an opponent discovers relevant information from public portions of a party's social media account, a court may be more likely to grant access to non-public content (see, for example, *Rhone*, 2016 WL 1594453, at *2-3 (requiring a plaintiff to provide a "Download Your Information" report from her Facebook account after the defendant discovered relevant information on public portions of her account page)).

However, counsel may attempt to shield non-public social media content through protective orders (see *Finkle v. Howard Cty., Md.*, 2015 WL 3744336, at *8 (D. Md. June 12, 2015), aff'd 640 F. App'x 245 (4th Cir. 2016); *Connolly*, 2018 WL 4462368, at *6; *Simply Storage,* 270 F.R.D. at 437*; Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009)).

For more on how to respond to document requests and subpoenas generally, see Practice Notes, Document Responses: Considerations in Preparing to Produce Documents (6-540-1711) and Subpoenas: Responding to a Subpoena (Federal) (1-503-1741).

AUTHENTICATING SOCIAL MEDIA

Social media evidence may be tangible (such as static screenshots) or consist of ESI. As with any other type of evidence, social media evidence generally must be authenticated under FRE 901 or self-authenticating under FRE 902 to be admissible (see Authenticating Social Media Under FRE 901 and Self-Authenticating Social Media Evidence Under FRE 902).

Counsel should carefully consider authentication issues during discovery, and whether a forensic expert may be needed to authenticate social media evidence. Counsel also should minimize the risk of authentication challenges at the outset of discovery by proper collection and production of:

- The devices utilized during the creation or use of the social media content.
- Social media metadata (which can be done with the assistance of a vendor or collection software).

(See Preservation.)

Authenticating Social Media Under FRE 901

Because evidence may be authenticated in many ways, federal courts have followed varying approaches to authentication challenges in the context of social media under FRE 901(b) (*United States v. Vayner*, 769 F.3d 125, 126-33 (2d Cir. 2014) (reversing a conviction based on an unauthenticated page of the defendant's alleged profile on a Russian social networking site akin to Facebook)). For example:

- The US Court of Appeals for the Third Circuit held that a defendant's Facebook chat messages, which Facebook gave to the government directly, were authenticated under FRE 901 in part because each of the four witnesses who participated in the chats testified about them, some of the witnesses had met the defendant in person as a result of the chats and could identify him in court, the defendant's testimony showed he owned the Facebook account in question, and biographical information on the page matched that of the defendant (*United States v. Browne*, 834 F.3d 403, 439-442 (3d Cir. 2016); see also *United States v. Barnes*, 803 F.3d 209 (5th Cir. 2015) (Facebook messages were authenticated in part because a witness testified that she had seen the defendant using Facebook and she recognized the account and his style of communicating from the messages)).
- The US Court of Appeals for the Fifth Circuit held that photographs on a defendant's Facebook page were not properly authenticated because a "photograph's appearance on a personal webpage does not by itself establish that the owner of the page possessed or controlled the items pictured" (*United States v. Winters,* 530 F. Appx. 390, 395-96 (5th Cir. 2013); see also *Vayner*, 769 F.3d at 131 (the defendant's name, photograph, and some details about his life on a printed profile page was insufficient to establish that he had actually created the profile or was responsible for its contents)).
- The US Court of Appeals for the Tenth Circuit held that Facebook messages were authenticated because the defendant failed to adequately challenge the authenticity of the messages, and the district court had properly admitted the messages as statements of a party opponent at trial (*United States v. Brinson,* 772 F.3d 1314, 1320-21 (10th Cir. 2014)).
- The US Court of Appeals for the Eleventh Circuit held that the district court had properly admitted a YouTube video into evidence because the government presented ample circumstantial evidence through the testimony of various witnesses identifying the individual in the video as the defendant, establishing where and when the video was recorded, and identifying the specific rifle and ammunition in question in the video. Because the government did not make the video, but merely found it on YouTube, it was not required to authenticate the video by offering evidence regarding the integrity of the recording equipment, the competence of the person taking the video, or whether the video was edited. (*United States v. Broomfield*, 591 Fed. App. 847, 851-52 (11th Cir. Dec. 3, 2014).)
- The Eleventh Circuit also held that Facebook comments were sufficiently authenticated where the defendants admitted that they controlled the account and made posts that were ascribed to them (*Stout by Stout v. Jefferson Cty. Bd. of Educ.*, 882 F.3d 988, 1008 (11th Cir. 2018)).
- A US district court held that a plaintiff's testimony about photographs posted on an Instagram account and the name associated with the account could authenticate the account, because the plaintiff knew the alleged account holder (*Diperna v. Chicago Sch. of Prof'l Psychology,* 222 F.Supp.3d 716, 723 (N.D. Ill. 2016)).
- A US district court held that statements made by a plaintiff on her Facebook page were authenticated by her deposition testimony and admissible as a party admission under Federal Rules of

Evidence (FRE) 801(d)(2), 901(a), and 901(b)(1) (*Targonski v. City of Oak Ridge*, 2012 WL 2930813, at *10 (E.D. Tenn. July 18, 2012)).

Self-Authenticating Social Media Evidence Under FRE 902

Social media evidence also may be self-authenticating under FRE 902. For example, the US Court of Appeals for the Fourth Circuit held that screenshots of Facebook pages and YouTube videos retrieved from a Google server were self-authenticating business records under FRE 902(11) where they were accompanied by appropriate certifications from Facebook and YouTube records custodians (*United States v. Hassan,* 742 F.3d 104, 132-34 (4th Cir. 2014); but see *Browne*, 834 F.3d at 433-6 (Facebook messages were not business records and therefore not self-authenticating under FRE 902(11)).

Additionally, depending on the circumstances and the collection method, some social media evidence may be self-authenticating under either:

- FRE 902(13), which applies to records generated by an electronic process or system.
- FRE 902(14), which applies to data copied from an electronic device, storage medium, or file.

To be self-authenticating under these rules, social media evidence must meet certain requirements and be accompanied by the appropriate certification. For more information, see Practice Note, E-Discovery: Authenticating Electronically Stored Information (W-002-6960). For sample certifications under these rules, see Standard Documents, FRE 902(13) Certification of Authenticity for Records Generated by an Electronic Process or System (W-012-7919) and FRE 902(14) Certification of Authenticity by Process of Digital Identification (W-015-0933).

Although FRE 902(13) and FRE 902(14) are intended to reduce the expense and inconvenience of establishing authenticity through the testimony of a foundation witness, the rules do not restrict a party from establishing authenticity of social media evidence on other grounds (see 2017 Advisory Committee Notes to FRE 902(13) and FRE 902(14)).

For more examples of authentication methods for social media, see E-Discovery: Authenticating Common Types of ESI Chart (W-003-7939).

SOCIAL MEDIA AT TRIAL

Social media can play a large role at trial. As with the investigation of parties, witnesses, and claims, counsel should explore the use of social media when selecting a jury panel. Counsel also should pay attention to the jurors' use of social media during trial and deliberations.

RESEARCHING JURORS ON SOCIAL MEDIA

Counsel can learn important information about prospective jurors, including any potential biases, by examining their:

- Educational and professional backgrounds on sites like LinkedIn.
- "Likes" and followed pages on sites such as Facebook.
- General social media activity, which may indicate whether prospective jurors are likely to seek information about the case outside of the trial record.

However, the parameters for social media investigation are more narrowly applied with respect to jurors and potential jurors than to adverse parties and witnesses (see Pre-Litigation Investigation). For example, the American Bar Association (ABA) issued an opinion:

- Restricting lawyers to searching only the public content of prospective jurors' social media accounts.
- Prohibiting lawyers from connecting with or following a juror or potential juror under any circumstances.

(See ABA Standing Committee on Ethics & Professional Responsibility, Formal Op. 466, Lawyer Reviewing Jurors' Internet Presence (Apr. 24, 2014).)

Lawyers should be cautious with social media platforms like LinkedIn, which may alert jurors that their profile and public content have been viewed. In some jurisdictions, this may be interpreted as inappropriate, unethical, and impermissible juror contact. (See 2017 NYSBA Social Media Ethics Guidelines, No. 6.B and cmt., at 30-32).

Counsel also should ensure compliance with any specific local or judge's rules or orders applicable to social media research on jurors. At least one court has expressed concern that allowing counsel to conduct social media research on potential and empaneled jurors could facilitate improper personal appeals to particular jurors, compromise the jury verdict, and compromise the jurors' privacy. That court therefore considered exercising its discretion to impose a ban against all internet research on the venire or the empaneled jury until the end of trial, a ban to which the parties ultimately agreed. (See *Oracle Am., Inc. v. Google Inc.*, 172 F.Supp.3d 1100, 1101-04 (N.D. Cal. 2016).)

MONITORING JURORS' USE OF SOCIAL MEDIA

Jurors' misuse of social media during trial is a growing problem that has the potential to undo extensive trial preparation work by resulting in a mistrial or forming the basis for an appeal (see, for example, *United States v. Villalobos,* 601 Fed.Appx. 274, 275 (5th Cir. 2015); *United States v. Fields*, 2016 WL 215267, at *11-12 (D. Mass. Jan. 19, 2016); *United States v. Juror Number One*, 866 F. Supp. 2d 442, 452 n.14 (E.D. Pa. 2011); *In re Methyl Tertiary Butyl Ether (MTBE) Products Liab. Litig.*, 739 F. Supp. 2d 576, 610 n. 215 (S.D.N.Y. 2010) (discussing the "recurring problem" and consequences of social media and internet use by jurors)).

Given the potentially severe consequences, counsel should consider monitoring jurors' use of social media by regularly (and ethically) checking the jurors' social media accounts throughout a trial and deliberations. Although a lawyer who becomes aware of a juror's improper use of social media may be tempted to stay quiet if the juror favors the lawyer's client, some bar associations, including the ABA, require lawyers who observe a juror's misconduct in public social media posts to report it to the court (see ABA Standing Committee on Ethics & Professional Responsibility, Formal Op. 466, Lawyer Reviewing Jurors' Internet Presence (Apr. 24, 2014)).

If jurors' social media use and abuse is a concern or a case is particularly high-profile, counsel may consider asking the court to:

- Instruct the jurors, at multiple points before and during trial, to avoid social media use, and explain the consequences of violating the instruction, such as being held in contempt.

- Require the jurors to take an oath to refrain from social media use during the pendency of the trial.

For examples of jury instructions warning jurors about their use of social media, see *United States v. Fumo*, 655 F.3d 288, 304-06 (3d Cir. 2011), as amended (Sept. 15, 2011); *United States v. Feng Ling Liu,* 69 F.Supp.3d 374, 377 (S.D.N.Y. 2014); *OneBeacon Ins. Co. v. T. Wade Welch & Associates,* 2014 WL 5335362, at *1-11 (S.D. Tex. Oct. 17, 2014); and *Toshiba Corp. v. Imation Corp.*, 2013 WL 7157854, at *10 (W.D. Wis. Apr. 5, 2013).

04-19