Technology - Sword or Shield
TECHNOLOGY - SWORD OR SHIELD

The digital world offers bountiful opportunities for disputing liability theories and damages from sources such as CSA scores, Fitbit information, ECM data, DriveCam video and social media. While gathering and preserving data pre-suit is difficult, using it at trial presents unique challenges. This session explores methods to ensure digital data will be both admissible and effectively utilized at trial.

I. Collecting Digital Evidence

A. General Duty of Attorneys

Social media users, both plaintiffs and employees alike, with online messaging and cell phone apps, Internet blogs, and social networking websites - like LinkedIn, Facebook, Twitter, Google, YouTube, Pinterest, and Instagram - are publishing electronic biographies and sharing information for public consumption. With respect to the client-lawyer relationship, every attorney has an ethical duty to be competent in the practice of law. Per, Rule 1.1 of the ABA Model Rules of Professional Conduct, competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation, and maintaining the knowledge. Comment 8 to Rule 1.1 requires lawyers to “keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.”

There is a growing trend in jurisdictions to impose an ethical duty on attorneys to have general knowledge of social media. The New Hampshire Bar Association Ethics Committee has advised lawyers that they: “have a general duty to be aware of social media as a potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation.” In Ethics Opinion No. 371, the D.C. Bar acknowledged the applicability of social media to the practice of law and emphasized the importance for lawyers to understand the basic components. In particular, the
D.C. Bar opined that, a lawyer’s ignorance or disregard of social media and other modern technologies may create the potential for ethical misconduct. This includes violating Rule 1.1 regarding competent representation. The Commercial and Federal Litigation Section of the New York State Bar Association concluded that an attorney cannot be sufficiently competent without a working knowledge of the benefits and risks associated with the use of social media. See N.Y St. Bar. Ass’n Com. & Fed. Litig. Sec., Social Media Ethics Guidelines (2015).

To be ethically compliant and avoid potential malpractice, attorneys must understand digital technology, whether or not they use the technology themselves when providing legal services.

B. **Pre-Suit - What to Preserve**

A legal hold is a mechanism to notify potential custodians of records, internally or externally, to preserve information, digital or otherwise, in anticipation of litigation. Litigation hold letters can be used offensively or defensively. The purpose is to avoid the destruction of potentially useful or relevant evidence in pending or future litigation. Events that may trigger the duty to preserve include: knowledge of an accident; receipt of a claim letter; service of a lawsuit; notice of a product malfunction; receipt of a subpoena; initiation of a regulatory investigation.

The Advisory Committee’s Notes to the 2015 amendment to Federal Rule of Civil Procedure 37(e) provide some guidance to the preservation duty of litigants. It states:

> Courts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant. A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation, however, so that the scope of information that should be preserved may remain uncertain.
In general, Courts have defined the preservation duty with a discoverability standard. The scope of discovery varies from jurisdiction to jurisdiction. The Federal Rule of Civil Procedure 26(b)(1), “Scope of Discovery in General,” states:

Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

Federal Rule of Civil Procedure 26(b)(2)(B), “Specific Limitations on Electronically Stored Information,” provides:

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Determining which custodians have a preservation duty depends on the facts of the accident or dispute. The duty to preserve typically applies to “key players” within a company, usually the decision-making personnel. The group can also include lower-level employees that have unique and relevant knowledge of the case’s facts. In Consolidated Aluminum Corp. v. Alcoa, Inc., 244 F.R.D. 335, 341 (M.D. La. 2006), the court found that a “plant level employee” was determined to be such a key player. The defendant argued that it did not instruct a particular employee to preserve his e-mails because of his lack of involvement in the investigation and his minimal interaction with decision making personnel. The court concluded, however, that defendant
previously argued that the employee’s knowledge of the relevant events was “critical to [defendant’s] defense and to its counterclaim.”

C. Ethical Concerns with Accessing Claimant’s Digital Data

Many social media services - such as LinkedIn and Facebook - notify a user when someone reviews profile. Ethical concerns exist about accessing social media of claimant. Model Rule of Professional Conduct 4.2, prohibits attorneys from communicating with person known to be represented by attorney about subject matter of representation. Looking at a public website of a represented party is not considered a communication, but communications made through social media are typically prohibited.

D. Pitfalls with Deleting Material

Deleting of material can lead to the possibility of sanctions. A recent Virginia case, Lester v. Allied Concrete Nos. CL.08-150, CL09-223 (Va. Cir. Ct. Sept. 1, 2011). Illustrates this point. The plaintiff’s counsel instructed his client to delete social media photos and “clean up” his Facebook account. Defense counsel had already obtained and preserved copies. The defendant also hired a forensic expert to examine IP logs from Facebook. This revealed the plaintiff had deleted sixteen (16) photographs. The plaintiff then testified he did not have Facebook account. The Court ordered a spoliation sanction to the attorney $542,000 and to the plaintiff of $180,000.

In a case in the Middle District of Florida, U&I Corp. v. Advanced Medical Design, 251 F.R.D. 667, 673 (M.D. Fla. 2008), the defendant company was sanctioned for failing to document its efforts to locate and produce emails contained on home personal computers of its employees.

II. Discoverability of Digital Evidence

A. Discovery Problems with Subpoenas

Congress passed the Stored Communications Act (“SCA”) because “the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.” Quon v. Arch
Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008). The SCA governs the circumstances under which electronic data service and storage providers may disclose customers’ data. The SCA has provided a statutory shield to social media providers, and hindered the ability to obtain useful information via subpoena.

In Crispin v. Christian Audigier, 717 F.Supp.2d 965 (C.D. Cal. 2010), discovery was sought about a party via subpoenas to Media Temple, Facebook and Myspace. The court quashed defendants’ subpoenas because the social media sites were considered electronic communication services (ECS) under the SCA. The court held that the social media sites were ECS providers under the SCA with respect to wall posting and comments and that such communications were electronic storage and inherently private. The providers could not divulge the contents of any communication carried or maintained on that service and could not divulge the contents of communication in electronic storage. The court quashed subpoenas to Media Temple, Facebook, and MySpace to the extent that they sought private messaging. Concerning Facebook wall posts and MySpace comments, the court vacated the lower court’s decision for an insufficient record about privacy settings of the subject social media accounts.

In Juror Number One v. Superior Court, 206 Cal.App. 4th 854 (2012), the court ruled that protection under the SCA applies only to attempts by the court or real parties in interest to compel the social media provider to disclose information, not to compel the person who posted the material to disclose.

**B. Discovery Requests Concerning Digital Data/Social Media**

Increasingly, courts allow at least some form of discovery of social media and digital evidence. Common grounds for denial of a motion to compel production of such evidence or allowance of a motion for a protective order is that the request is overly broad. A discovery
request that is drafted without specificity will likely be deemed overbroad and unduly burdensome. For example, asking for all information posted to social media.

In Ford v. United States, CIV. A. DKC11-3039, 2013 WL 3877756 (D. Md. July 25, 2013), the defendants moved to compel discovery from both the plaintiff and the plaintiff's expert of “‘any documents [,] postings, pictures, messages[,] or entries of any kind on social media within the covered period relating to [c]laims by Plaintiffs or their [e]xperts.’” The court denied the request to compel, ruling that the request was “not narrowly tailored” and “does not describe the categories of material sought; rather, it relies on Plaintiffs to determine what might be relevant.”

Discovery requests seeking social media and digital evidence should be crafted with specificity and impose as little a burden as possible on the producing party.

III. Use at Digital Evidence Trial - Admissibility Concerns and Juror Misconduct/Vetting

A. Authentication

Authentication is the identification of evidence at trial or another adjudication. Authentication and identification are “special aspects” of relevancy. Fed.R.Evid. 901(1), advisory committee’s note (“Authentication and identification represent a special aspect of relevancy.”) In order to authenticate evidence, the proponent of the evidence must offer sufficient evidence “that the matter in question is what the proponent claims” i.e. the evidence is “authentic.” Id. For example, most Courts will admit a photograph into evidence only after there is some testimony from a witness demonstrating that the photograph fairly and accurately depicts what the proponent of the photograph suggests it does. The jury can then assess the credibility of the witness’ testimony and, ultimately, the weight to be given to the photograph.

Authentication is governed by Federal Rule of Evidence 901, and in many instances circumstantial evidence may be the key to successful authentication of social media evidence.
Federal Rule of Evidence 901(b) sets forth examples of evidence that satisfy the general requirement of authentication. It reads:

Rule 901 – Authenticating or Identifying Evidence

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement:

(1) Testimony of a Witness with Knowledge. Testimony that an item is what it is claimed to be.

(2) Nonexpert Opinion About Handwriting. A nonexpert’s opinion that handwriting is genuine, based on a familiarity with it that was not acquired for the current litigation.

(3) Comparison by an Expert Witness or the Trier of Fact. A comparison with an authenticated specimen by an expert witness or the trier of fact.

(4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

(5) Opinion About a Voice. An opinion identifying a person’s voice — whether heard firsthand or through mechanical or electronic transmission or recording — based on hearing the voice at any time under circumstances that connect it with the alleged speaker.

(6) Evidence About a Telephone Conversation. For a telephone conversation, evidence that a call was made to the number assigned at the time to:

(A) a particular person, if circumstances, including self-identification, show that the person answering was the one called; or

(B) a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.
(7) *Evidence About Public Records.* Evidence that:

(A) a document was recorded or filed in a public office as authorized by law; or

(B) a purported public record or statement is from the office where items of this kind are kept.

(8) *Evidence About Ancient Documents or Data Compilations.* For a document or data compilation, evidence that it:

(A) is in a condition that creates no suspicion about its authenticity;

(B) was in a place where, if authentic, it would likely be; and

(C) is at least 20 years old when offered.

(9) *Evidence About a Process or System.* Evidence describing a process or system and showing that it produces an accurate result.

(10) *Methods Provided by a Statute or Rule.* Any method of authentication or identification allowed by a federal statute or a rule prescribed by the Supreme Court.

A number of the examples set forth in 901(b) can apply to authentication of social media and digital evidence.

1. **Testimony of Witness With Knowledge**

The owner of the social media page may identify the page, and further authenticate the statement at issue as his post or comment. In the alternative, the proponent may also be able to authenticate a social media post through a witness who watched the owner submit or place the post. Photographs and text entries, including those posted digitally, may be authenticated by any witness who can testify that they fairly and accurately depict within the witness’ personal knowledge. A Facebook page print-out can be authenticated by a witness who went to the website using the assigned URL, viewed the information, and that the print-out fairly and accurately
represents what he or she saw at the website. **ACTONet, Ltd. v. Allou Health & Beauty Care, 219 F.3d 836, 848 (8th Cir. 2000).**

2. **Comparison By Trier or Expert Witness**

Comparisons by both expert witnesses and the trier of fact itself are permitted. Fed.R.Evid. 901(b)(3). To determine if they came from the same source, an expert or the trier of fact can compare “known” examples with the evidence. For instance, the defendant’s Facebook page versus a print-out of the defendant’s Facebook page from another date. The trier of fact can conclude that the Facebook page in question features the same profile picture or biographical information as an already authenticated print-out from the defendant’s Facebook page.

3. **Distinctive Characteristics**

Authentication may be established through an item’s distinctive appearance, content, substance, internal patterns or other distinctive characteristics. For example, a social media post may contain a unique signature or sign-off. Repeated misspellings of certain words may also provide an adequate to demonstrate the author made the post.

Courts can be skeptical of such methods of authentication, however. In **Griffin v. State, 10 A.3d 415 (Md Apr. 2011),** the Court determined the proponent of the evidence could not show that the author of a MySpace post based solely on a photo, a location, and a date of birth. The court was concerned that someone else could have posted the comments. The court stated that “authenticating electronically stored information presents a myriad of concerns because ‘technology changes so rapidly’ and is ‘often new to many judges.’” **Id.** at 423. It “requires greater scrutiny of ‘the foundational requirements’ than letters or other paper records, to bolster reliability.” **Id.**

B. **Digital Resources Before, During and After Jury Selection**
Digital resources can be used to review juror’s backgrounds during voir dire and to monitor juror misconduct during and after trial. Increasingly, trial judges are instructing jurors to refrain from communication about their jury service or the pending case. Trial judges commonly instruct jurors avoid conducting personal investigation about the parties and issues involved in the case, including research on the Internet. Jurors have discussed trial issues on social media and in some cases solicited access to witnesses and litigants on social media. There are infamous examples of jurors revealing prejudices or a relationship with a party that were concealed during voir dire.

There are ethical considerations surrounding the scope of review and monitoring an attorney, and his/her agents, can perform. ABA Formal Opinion 466, the Standing Committee on Ethics and Professional Responsibility opines that reviewing juror’s internet presence or passive review of social media site is permissible, but requesting to friend a juror is a prohibited communication under Rule of Professional Conduct 3.5(6). Model Rule 3.5 addresses communications by attorneys before, during, and after trial with jurors. The rule states:

A lawyer shall not:

(a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law;

(b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order;

(c) communicate with a juror or prospective juror after discharge of the jury if:

(1) the communication is prohibited by law or court order;

(2) the juror has made known to the lawyer a desire not to communicate; or

(3) the communication involves misrepresentation, coercion, duress or harassment.
Unless authorized by law or court order, an attorney may not under Model Rule 3.5(b) communicate with a potential juror leading up to trial or any juror during trial. See, In re Holman, 286 S.E.2d 148 (S.C. 1982) (communicating with member of jury selected for trial of lawyer’s client was “serious crime” warranting disbarment). A lawyer may not, through a third-party, do what the lawyer is directly prohibited from doing. Model Rule 8.4(a); see also In re Myers, 584 S.E.2d 357 (S.C. 2003) (improper for prosecutor to have a lay member of his “jury selection team” phone venire member’s home); cf. S.C. Ethics Op. 93-27 (1993) (lawyer “cannot avoid the proscription of the rule by using agents to communicate improperly” with prospective jurors).

ABA Formal Opinion 466 suggests that reviewing juror’s internet presence or passive review of social media site is permissible, but requesting to friend a juror is a prohibited communication under Rule of Professional Conduct 3.5(6). The Committee concluded that a lawyer may not personally, or through another, send a social media access request to a juror. An access request should be considered an active review of the juror’s electronic social media by the lawyer. This would be the type of ex parte communication prohibited by Model Rule 3.5(b)(6).