#GOTCHA!: LITIGATION STRATEGIES FOR THE EFFECTIVE AND ETHICAL USE OF SOCIAL MEDIA EVIDENCE

June 22 – 25, 2014

Amy Schmidt Jones
Michael Best & Friedrich LLP
Milwaukee, Wisconsin

Margaret L. Wu
University of California
Oakland, California

I. WHAT IS SOCIAL MEDIA?

A. Social media has been described as the collection of web-based services that allow individuals to:

1. Construct a public or semi-public "profile" within a bounded system;
2. Identify a list of other users with whom they share connections; and
3. View and traverse their connections and connections made by others within the system.[1]

B. Essentially, social media is made up of a group of interactive, Internet-based applications that enable users to connect with others, broadcast information and ideas to audiences, and receive information.

1. Social media sites are participatory and allow users significant editorial control.
    a. Most social networking sites allow users to:
        i. Create personal profiles;
        ii. Write status updates or blog entries;
        iii. Post photographs, videos, and audio clips;
        iv. Send and receive private messages; and
        v. Link to the pages of other users.
2. Social media sites compare to traditional "Web 1.0" content, which is produced, edited, and maintained by the website's creator with no input from viewers.

C. Social media is essentially a form of cloud computing.

1. The data created in or uploaded to a user's account is hosted by the social media platform and maintained by a third party.
2. Users do not actively maintain the data created in or uploaded to their social media accounts on their own servers.
3. As a result, an individual's social media content is subject to third party policies and practices.

D. There are hundreds of different social media sites used throughout the world based on any imaginable community or common interests. Some of the most popular social media sites include:

[1] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER MEDIATED COMM. 210 (2007).

1. Facebook:
    a. The most popular social media network, founded in 2004.
    b. At the time of its founding, Facebook primarily catered to students.
        i. Originally available only to Harvard students, then to students at other Ivy League universities, then to students at any university or high school, and now anyone over age 13 can join and create an individual profile.
    c. Over one billion active monthly users worldwide.
    d. Allows users to create individual profiles and self-select an audience for the content shared on those profiles.
2. Google-plus:
    a. Described by Google as a "social layer" that enhances Google's other online properties.
    b. Permits users to share content with others in their "Circles," browse ongoing conversations about particular topics on various "Communities" pages, and engage in free video conference calling using the "Hangouts" feature.
    c. Second-largest social networking site after Facebook.
3. Twitter:
    a. A micro-blogging platform which allows users to post messages, or "tweets," of up to 140 characters.
        i. Popular platform for sharing breaking news and real-time updates.
        ii. Cross between instant messaging and blogging.
    b. More than 650 million registered users since 2006.
4. LinkedIn:
    a. The world's largest professional networking social media platform.
    b. LinkedIn profiles focus on users' education and work experience.
    c. Allows users to broadcast their professional experiences and goals and connect with others to build professional networks.
    d. More than 200 million active users worldwide.
5. Tumblr:
    a. Combines a micro-blogging platform with other social media capacities.
    b. Allows users to essentially post anything they want to their personal sites.
        i. Users can share multiple media types: Full-length text blog posts, photos, videos, songs, or hyperlinks to other websites.
            (a) Tumblr is visual focused. Re-blogged pictures are the most prevalent content posted to Tumblr sites.
            (b) Compare to Twitter, which limits users' posts to text.
    c. Acquired by Yahoo! In 2013 for $1.1 billion.
6. YouTube & Vimeo:

a. Video-hosting and watching websites.

b. YouTube, founded in 2005, boasts more than one billion unique user visits each month.

c. According to YouTube, 100 hours of video are uploaded to the site every minute.

7. Instagram & Flickr:

a. Photo and video sharing applications that allows users to share images (rather than text) on a variety of social networking sites.

b. Flickr popular among photographers who enjoy photo editing, whereas Instagram features amateur, un-edited photos taken on individual users' smartphones.

c. Known as the "visual versions of Twitter."

8. Pinterest:

a. Users share project ideas, recipes, and other images on their personal boards.

b. Browsing allows users to explore other users' ideas and images and "pin" ideas to their own boards.

9. Match.com:

a. Launched in 1995, Match.com pioneered the online dating industry.

b. Connects singles looking for relationships to other singles by allowing users to share photos and a personal profile and browse for other singles in the same geographic region.

c. Operates in twenty-four countries and in fifteen languages.

10. Tinder:

a. First launched at a University of Southern California party.

i. Officially released in September 2012.

ii. Backed by the same company that owns Match.com.

iii. Popular on college campuses.

b. Location-based dating tool that facilitates communication between mutually interested users.

c. Tinder gathers users' basic information and matches users who are most likely to be compatible based on geographic location, number of mutual friends, and common interests.

i. Users can use chat information to connect before meeting in person.

11. FourSquare:

a. Location-based social media platform which allows users to "check in" at venues using their mobile devices and broadcast their locations to other users.

II. SOCIAL MEDIA USAGE IN HIGHER EDUCATION

A. Students and social media:

1. Most students today fall within the category of "Digital Natives."

a. According to Marc Prensky, who coined the term in 2001, Digital Natives "think and process information fundamentally differently from their predecessors" and speak "an entirely new language."[2]

b. Many college students expect communication with academic and extra-curricular programs to mimic the communication in the rest of their lives, and universities and their faculty must deal with this phenomenon

2. In one survey, nearly ninety-eight (98%) of college-aged students (18-28) said that they use social media to interact with friends. Only twenty-six (26%) of students said they use social media for learning.[3]

3. Facebook is the favorite site among college-aged students.

   a. However, as more older adults (25+) join Facebook, college-aged students are seeking out new social media platforms.

   b. Twitter and Instagram have been gaining ground on Facebook among this age demographic.

      i. As many as 1 in 3 college students are actively using Twitter.

   c. Blend: "Share, Snap, Score."

      i. New social networking platform exclusively for undergraduate students.

         (a) Went live in September 2013.

         (b) Now being used on more than 1,000 college campuses, with more than 50,000 active daily users.

      ii. Users can share photos and win gift cards that are redeemable for college-focused retailers and brands.

         (a) Blend posts a theme relevant to its college audience each day.

            1. Examples include "Tailgate Saturday," and "Library Shenanigans"

         (b) Student users post photos on the site that relate to the theme of the day.

         (c) Photos receive "snaps," or likes, which can be redeemed for prizes.

      iii. Plans in coming months to enhance Blend by adding additional interactive features, while still maintaining the college-student-only audience that has made it popular.

4. What about homework?

   a. According to one study, freshmen women spend nearly half their day engaged in some form of social media use, and such intense use of social media negatively impacts grades.

5. The technology-plagiarism link.

   a. On the Internet, access to information is instantaneous, making it increasingly easier for students to plagiarize others' work as their own.

   b. Social media, which permits users to share information to a wide audience and connect with their "friends" easily, may facilitate academic dishonesty as college students are able to share plagiarized material freely.

---

[2] Marc Prensky, *Digital Natives, Digital Immigrants*, http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (last visited Apr. 22, 2014).
[3] Bellarmine A. Ezumah, *College Students' Use of Social Media: Site Preferences, Uses, and Gratifications Theory Revisited*, http://ijbssnet.com/journals/Vol_4_No_5_May_2013/3.pdf (last visited Apr. 22, 2014).

B. Faculty members and social media.[4]

1. The level of personal use of social media among faculty (70.3 percent) mirrors that of the general public
    a. Unsurprisingly, social media usage correlates with age.
        i. Eighty-seven (87) percent of faculty under age 35 use social media.
        ii. Sixty-three (63) percent of faculty over age 55 use social media.
    b. There also appears to be a relationship between the rate of personal social media use and the academic discipline of a faculty member.
        i. Seventy-four (74) percent of faculty who teach in Humanities and Arts use social media.
        ii. Sixty-four (64) percent of faculty in Natural Sciences use social media.
    c. Facebook is the most-visited site for personal purposes.
    d. The need for university policies to guide faculty members' social media usage is growing as more and more faculty plug in.
        i. The recent experience of the Kansas Board of Regents is just one example of how universities are trying to control faculty use of social media – and what obstacles universities may face in the process.
            (a) In September 2013, the University of Kansas suspended a journalism professor over an inappropriate comment he posted to his personal Twitter account.
            (b) The Board of Regents quickly adopted rules that made "improper use of social media" a fireable offense.
                1. Rules quickly came under fire as threatening academic freedom.
                2. In March 2014 the Board released a new draft social media policy that would give faculty broader freedom to communicate online.
                    a. New draft defines improper social media as including speech not protected by the First Amendment.
        ii. American Association of University Professors' 1940 Statement of Principles on Academic Freedom and Tenure states that faculty members "should be free from institutional censorship or discipline," but is also mindful that faculty sometimes speak as individuals and not representatives of their institutions
2. Fifty-five (55) percent of faculty use social media in a professional context outside of teaching.
    a. LinkedIn is the most-visited site for professional purposes.
3. Only forty-one (41) percent of faculty use social media in the classroom.
    a. Blogs are the most-used sites for teaching, followed by podcasts.
    b. Facebook, the most often accessed social media site for personal use, is the least used site for teaching purposes.

[4] Pearson Learning Solutions & Babson Survey Research Group, *Social Media for Teaching and Learning*, 2013, *available at* http://www.pearsonlearningsolutions.com/assets/downloads/reports/social-media-for-teaching-and-learning-2013-report.pdf#view=FitH,0.

c. As Digital Natives continue to fill university classrooms, professors will have to decide whether they must increase the role social media plays in their lesson plans.

4. Just like students, faculty members report that social media is distracting and results in longer working hours and more stress.

   a. Many faculty members recognize the potential for social media technology to be a distraction, rather than an empowering component of teaching.

C. Universities and social media.

1. Admissions offices often use social media as a recruitment tool.

   a. Appeal to millennial generation students who expect real-time interaction with their prospective universities.

   b. Students use social media to research schools, so schools understand that they must have a stronger online presence than ever before.

      i. University Pages on LinkedIn launched in 2011.

         (a) Schools can set up profiles, much like individual users do on other social media platforms.

         (b) Regular updates about campus news and activities.

         (c) Platform for prospective students to submit questions to schools.

         (d) Allows users to search for alumni and form networks.

   c. Many admissions officers also use Google to search for applicants or visit their social media profiles.

      i. Content on applicant's social media site may negatively impact his or her chance of being admitted.

2. Twitter and other micro-blogging sites permit universities to create live, up-to-the-minute marketing and coverage of on-campus events.

3. A challenge for universities that utilize social media for recruitment and marketing is the openness of social media platforms.

   a. Universities can quickly lose control over the content posted to "official" social media pages if they are not monitored closely.

      i. On a higher education campus, duplication of presence through social media sites by the many different campus programs can create confusion.

      ii. Universities need to consider policies aimed at guiding what school groups are allowed to have "official" presence on social media.

         (a) What groups are allowed to use official school logos on their profiles?

         (b) Does a school official have final say over content?

   b. Visitors to university social media profiles can easily post comments that may be detrimental to the university's mission.

III. THE ROLE OF SOCIAL MEDIA EVIDENCE IN LITIGATION

A. Parties involved in litigation are increasingly looking to social media content as potential sources of evidence, including:

1. Current and former names, phone numbers, addresses, and email addresses associated with a user's account.
2. An individual's employment status.
3. Demographic information shared by the user in an "about me" section, including education, birthdate, family members, favorite quotes, gender, hometown, political views, and religious views (to name a few).
4. Physical locations the user has visited or "checked into."
5. Photos, videos, or other posts made by the user.
6. Sent and received "private" messages or chat conversations with other social media users.
7. Lists of individuals who have liked a user's posts, or who have RSVP'd to events organized by the user.
8. Photos, videos, or other posts made by another person to the user's account or which the user "liked."
9. Events the user has been invited to attend.
10. Date and time of a user's log-ins or active social media sessions.
11. A list of IP addresses used to log into a user's social media account.
12. Credit card information provided by a user to pay for special social media applications ("apps").

B. Such evidence can be useful in litigation for many purposes.

1. Status updates, postings, and photos may establish motive or intent or demonstrate a party's knowledge of a particular event.
2. Social media content may contain contradictory statements, character evidence, or other evidence that can be used to impeach a witness.[5]

a. *People v. Liceaga* (Mich. Ct. App. 2009): Defendant admitted to shooting and killing friend, but claimed it was an accident.

i. Issue at trial was defendant's state of mind at the time of the shooting.

ii. Trial court allowed prosecution to introduce a picture of Defendant from his MySpace page that showed him holding the gun that was used in the shooting and displaying a gang sign.

iii. Defendant was convicted and Court of Appeals affirmed the use of the MySpace page as evidence.

b. *Mai-Trang Thi Nguyen v. Starbucks Coffee Corp.* (N.D. Cal. 2009): Employee was fired for engaging in inappropriate conduct and threatening co-workers, after which employee sued.

[5] Gregor Pryor, Joseph Rosenbaum, Douglas Wood & Stacy Marcus, eds., *Network Inference, A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon*, http://www.reedsmith.com/files/Publication/f7c1a768-c22c-4be5-823e-606cc6b9408a/Presentation/PublicationAttachment/2289c1ee-ddea-4c39-99ee-f35d71a0fce3/121221social-media_whitepaper.pdf (last visited Feb. 28, 2014).

i. Employee's MySpace page, which contained erratic statements and statements to the effect of "I thank GOD 4 pot 2 calm down my frustrations and worries or else I will go beserk [sic] and shoot everyone" was submitted as evidence.

ii. Court granted summary judgment to Starbucks.

3. A party's "friends," or list of social media contacts, may assist in identifying additional witnesses with relevant and discoverable information.

4. Learning that an identified witness is "friends" with a party might also expose potential biases of that witness.

5. In the context of employment termination disputes, a party might reveal his or her current employment status, which could determine what damages in the form of back pay, if any, are due to the party.

6. In the family law context, information and photos shared over social media might reveal information regarding a parent's fitness.

7. Because users often post about their thoughts and social activities, social media evidence can be particularly useful when a party has claimed physical and emotional injuries in a personal injury or worker's compensation case.

   a. *Romano v. Steelcase Inc.* (N.Y. Sup. Ct. 2010): Personal injury plaintiff claimed her injuries prevented her from running and horseback riding, thereby lessening her enjoyment in life.

      i. Publicly-accessible portions of plaintiff's Facebook and MySpace pages revealed that she maintained an active lifestyle and still traveled.

      ii. Defendant sought discovery of non-public portions of these pages to determine if they also revealed plaintiff's engagement in activities, thereby contradicting her claimed injuries.

      iii. Court allowed the discovery in light of plaintiff's claims.

   b. *Offenback v. L.M. Bowman, Inc.* (M.D. Pa. 2011): Plaintiff claimed that car accident prevented him from riding a motorcycle or being in traffic around other vehicles.

      i. Plaintiff's Facebook postings showed that he continued to ride motorcycles, including on trips to other states.

      ii. Court ordered plaintiff to turn over content from his Facebook account that related to his continued motorcycle use and thereby contradicted his claim.

   c. *Largent v. Reed* (Pa. Ct. Com. Pl. Nov. 18, 2011): Plaintiff claimed she suffered from depression and leg spasms and had to use a cane following a car accident.

      i. Plaintiff's public Facebook statuses and updates showed that she exercised at a gym and enjoyed time with family and friends.

      ii. Plaintiff compelled to produce her Facebook username and password because her Facebook content contradicted her claims.

IV. THE DISCOVERABILITY OF SOCIAL MEDIA CONTENT

A. Parties in litigation are entitled to discovery of all relevant, non-privileged information, and social media content is no different.

1. *EEOC v. Original Honeybaked Ham Co. of Ga.* (D. Colo. 2012): Explaining that the creation of social media is just like a litigant assembling "a file folder titled 'Everything About Me.'"

    a. If documents in that folder contain relevant information or may lead to the discovery of other relevant information, they are discoverable.

    b. The fact that this "About Me" folder exists in cyberspace – rather than in a traditional, handwritten journal – is inconsequential under the discovery rules.

2. This is true even when parties have "privacy" settings in place for their accounts which result in only their "friends" being able to see posted content.

    i. *Ledbetter v. Wal-Mart Stores, Inc.* (D. Colo. 2009): Court denied plaintiff's motion for a special protective order against defendant's subpoenas to various social media services and made clear that social media information merits no special treatment when it comes to discovery.

    ii. *EEOC v. Simply Storage Mgmt., LLC* (S.D. Ind. 2010).

        (a) Plaintiffs in an employment discrimination suit alleged depression and stress disorders, and defendant sought discovery of all social media content related to plaintiffs' emotions, feelings, or mental states and communications revealing the same.

        (b) Court permitted the discovery, rejecting plaintiffs' argument that the request infringed on privacy, even though plaintiffs had privacy settings in place.

            1. "Merely locking a profile from public access does not prevent discovery."

        (c) Court took the position that as with any other sensitive material produced in discovery, a social media user's privacy or confidentiality concerns can be dealt with through a protective order – but not through a shield forbidding social media discovery in the first place.

    iii. *Romano v. Steelcase, Inc.* (N.Y. Sup. Ct. 2010): Court flatly rejected plaintiff's privacy claim and stated that she could not hide behind "self-set privacy controls on a website" to block defendant from learning about how she leads her social life.

        (a) According to the court, plaintiff "knew that her information may become publicly available," despite the existence of privacy controls.

            1. Neither Facebook nor MySpace promise complete privacy in user content.

            2. With no promise of privacy from the social media providers, the court held that plaintiff's claimed expectation of privacy was "wishful thinking."

        (b) The whole point of social networking sites is for people to share personal information with others, so a social media user's protest of privacy during discovery will not get him/her very far.

    iv. *Patterson v. Turner Constr. Co.* (N.Y. App. Div. 2011): Relevant social media content is not shielded from discovery "merely because plaintiff used the service's privacy settings to restrict access."

    v. *Loporcaro v. City of New York* (N.Y. Sup. Ct. 2012): There is no guarantee that pictures and information posted to a social media site will remain private, *regardless of* a user's privacy settings.

        (a) "Private" is not the same as "not public."

(b) By sharing content with others via social media, even if only to a limited number of selected "friends," a user has no reasonable expectation of privacy with respect to social media content.

vi. Many social media providers even include disclaimers or terms of use policies on their sites warning users that they essentially post at their own risks, thereby further diminishing the viability of any privacy argument.

(a) Users must agree to Twitter's Terms of Service and Privacy Policy, which states that Twitter may preserve or disclose user information and explains that Twitter's servers "automatically record [user] information," including "IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information."

3. Because social media content is fair game in discovery, parties should thus not overlook the potential that social media content might reveal relevant information helpful in litigation.

4. If it appears that social media does contain relevant information, parties must consider how to obtain that evidence through discovery.

V. OBTAINING SOCIAL MEDIA CONTENT FROM THIRD-PARTY SOCIAL MEDIA PROVIDERS

A. The use of a Rule 45 subpoena to obtain information from a non-party social media provider presents challenges.

B. As a result of the Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq., absent a user's consent and authorization, most social media providers will not produce content, even in response to a subpoena.

1. Enacted as part of the Electronic Communications Privacy Act (ECPA) in 1986, the SCA is the primary federal statute governing the privacy of stored Internet communications.

2. SCA prohibits an entity that provides electronic communications services (ECS) or remote computing services (RCS) from disclosing the contents of its users' communications – whether voluntarily or under compulsion – without a search warrant, unless an exception is met.

a. The distinction between an ECS and an RCS is complex and creates difficulties for courts when applying the SCA.[6]

i. This is especially true because most network service providers are multi-functional, and a provider likely operates as an ECS sometimes and an RCS other times.

ii. That being said, the difference is important because the scope of privacy protections hinges on the distinction when it is a governmental entity making the demand.

b. ECS: Any service which provides users with the ability to send or receive wire or electronic communications, including email and text messages.

i. With respect to an un-opened e-mail, a provider is an ECS with respect to that message.

[6] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

c. RCS: Any service which provides the public with computer storage or electronic processing services, including an electronic bulletin board.

i. With respect to a received, opened, and read e-mail which has been saved to a folder, a provider is likely an RCS.

C. Application of the SCA to social media discovery.

1. SCA passed before the social media revolution, so there is no legislative history to guide courts with regard to the statute's intended application to social media content.

a. The SCA was specifically designed to apply to "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and . . . digitized networks."[7]

b. Modern social media providers do not fit easily within any of these categories, and Congress has not yet amended the SCA to deal with emerging technologies and the rising prevalence of Digital Natives.

2. Although few courts have addressed whether the SCA governs social media content, the leading cases have answered that question affirmatively.

a. *Crispin v. Christian Audigier, Inc.*(C.D. Cal 2010): Leading case analyzing whether social media providers are covered by the SCA.

i. Defendant sought the production of social media content, including communications between plaintiff and another individual, by subpoenaing Facebook and MySpace for such content.

ii. Court held that a social media provider constitutes an ECS and therefore granted plaintiff's motion to quash defendant's subpoenas.

(a) Since plaintiff had at least some privacy settings in place and profiles were not entirely available to the general public, the SCA prohibited Facebook and MySpace from producing the content in question, even with a subpoena.

b. *Ehling v. Monmouth Ocean Hosp. Serv.* (D.N.J. 2013): Court held that Facebook posts that are configured to be private are by definition not accessible to the general public and thus fall under the SCA.

c. For its part, Facebook *does* consider itself governed by the SCA, and Facebook will not respond to civil subpoenas seeking user content, absent user consent.

i. *See* http://www.facebook.com/help/133221086752707/.

(a) "the Stored Communications Act . . prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or a court order."

(b) "federal law does not allow private parties to obtain account contents (ex: messages, Timeline, posts, photos) using subpoenas."

d. Twitter has a stated policy of producing data only in response to legal process.

e. In its "Information for Law Enforcement" section, Instagram states that it is governed by the SCA and that a court ordered subpoena is required to compel Instagram to disclose user records, including photographs, photograph captions, and other electronic communication information.

[7] H.R. Rep. No. 99-647, at 18 (1986), *available at* http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/houserept-99-647-1986.pdf.

f. MySpace's policy speaks only to its willingness to comply with law enforcement requests in certain circumstances and says nothing at all about civil subpoenas.

D. Statutory Exceptions to the SCA's Prohibition.

1. Disclosure to the government pursuant to a warrant.[8]

2. Disclosure of *non-content*, basic subscriber information to civil litigants.

a. "Content" for purposes of the SCA means "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8)

i. The content of an e-mail message, for example, would include the subject and body text of the e-mail.

ii. The logs or subscriber information related to the sending, though, would not be content and thus could be freely shared without running afoul of the SCA.

iii. Examples of non-content information in the social media context include a subscriber's user name or a list of the times the subscriber logged into the social media platform.

b. Because of the SCA's carve-out for non-content subscriber information, social media providers that are subject to the SCA will at most only provide basic subscriber information in response to a civil subpoena (and absent authorized user consent).

i. Not only is this unlikely to produce much valuable evidence, but Facebook has particular rules regarding subpoenas.

ii. Facebook will only respond to a valid California state or federal subpoena, and subpoenas from proceedings taking place outside of California must be "domesticated."[9]

3. Disclosure pursuant to authorized user consent.

a. The SCA provides that to legally obtain content information, one must obtain "the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing services." 18 U.S.C. § 2703(b)(3).

b. *Ehling v. Monmouth Ocean Hosp. Serv.* (D.N.J. 2013): Plaintiff-employee friended co-worker on Facebook. Co-worker voluntarily provided employer with copies of postings made by plaintiff-employee on Facebook. Employer did not violate the SCA because of the authorized user exception: (1) access to communication in question was authorized; (2) by the user of the communication service (the plaintiff-employee); and (3) access was not coerced or provided under pressure.

4. Even if one of the statutory exceptions to the SCA is met (including authorized user consent), that only means that a service provider may *voluntarily* disclose the contents of electronic communications.

5. Significantly, the SCA does not contain any outright exception for disclosure pursuant to a civil subpoena. The service provider, if it is deemed subject to the SCA, still cannot be *compelled* to do so, even by bringing a civil action against the service provider.

a. Several courts have in fact held that social media providers subject to the SCA may not produce content records in response to a civil subpoena and cannot even be compelled by a court order to do so.

[8] 18 U.S.C. § 2703.
[9] *See* California Code of Civil Procedure § 2029.300.

i. *O'Grady v. Superior Court* (Cal. App. 4th 2006): "A subpoena is not enforceable if compliance would violate the SCA. Any disclosure violates the SCA unless it falls within an enumerated exception to general prohibition."

(a) The *O'Grady* court relied on the plain statutory language of the SCA.

(b) According to the court, "by enacting a number of quite particular exceptions to the rule of non-disclosure, Congress demonstrated that it knew quite well how to make exceptions to that rule," and yet Congress chose not to include any exception for disclosure pursuant to a valid civil subpoena.

(c) According to the Court, in enacting the SCA, Congress rationally concluded "that one seeking disclosure of the contents of email [or other online content] should direct his or her efforts to the parties to the communication and not to a third party who served only as a medium and neutral repository for the message."

ii. *In re Subpoena Duces Tecum to AOL, LLC* (E.D. Va. 2008): Quashing a subpoena issued by State Farm to AOL, seeking disclosure of the stored e-mails of two of its customers.

(a) The court held that receipt of a civil subpoena does not compel disclosure of materials covered by the SCA.

b. Note, however, that if a subpoena calls for production of records containing only "non-content" information, then the SCA does not bar enforcement, because non-content information is not protected by the SCA.

E. The SCA's prohibition only applies to an ECS or an RCS, not to individual users.

1. *Juror No. One v. Superior Court* (Cal. Ct. App. 2012): SCA only applies to attempts by a party to compel a social media provider to disclose social media content, not to attempts to compel the individual who actually posted the content to disclose.

2. Result: Most social media discovery occurs through individual users using the tactics discussed below rather than through social media providers because, as stated above, the SCA shelters covered providers from legal obligation to respond to civil subpoenas that seek content information. Even if an individual user provides his/her consent to the disclosure of content information, that only means that the social media provider may voluntarily disclose it.

VI. METHODS FOR OBTAINING SOCIAL MEDIA DISCOVERY FROM INDIVIDUAL USERS

A. Engage in informal discovery.

1. A Google search might reveal a party's publicly available social media content.

a. Many social media users do not know about – or do not set – privacy controls, so more of their content might be public than they think.

2. Despite its obvious limitations (private content will not be revealed), informal discovery may at least be helpful in developing a strategy for more formal discovery of social media content, with the added bonus that it is free.

B. Serve well-tailored discovery requests to obtain relevant private content.

1. Rule 34 requires "reasonable particularity" and Rule 26 requires that the information sought be relevant or likely to lead to the discovery of admissible evidence.

2. Courts often permit rather broad discovery of private social media content if the party seeking discovery can show that the publicly available content suggests that there is likely relevant private content.
    a. A discovery request for the production of social media content should thus show that the request is not a mere fishing expedition and instead seeks evidence that likely exists.
    b. Litigants should tailor social media discovery requests to specific time frames and, if possible, particular subject matters to maximize their chances of successfully obtaining the requested discovery.
        i. In an employment discrimination case, a request for social media content might properly be limited to posts made during the dates of employment or which reference the employment.
        ii. In a personal injury case in which the plaintiff claims loss of enjoyment, a discovery request might be limited to photos of plaintiff engaging in activities outside of the home or posts referencing social activities.
    c. *Howell v. The Buckeye Ranch, Inc.* (S.D. Ohio 2012): Court denied motion to compel production of plaintiff's log-in information and password for her social media sites because the discovery request was not limited to only social media content relevant to the claims and defenses in the case.
    d. *Mailhoit v. Home Depot USA, Inc.* (C.D. Cal. 2012): Request for "any profiles, postings or messages" and for "any pictures of Plaintiff" from any social media site in a seven-year period rejected by court as overly-broad.
    e. *Tompkins v. Detroit Metro. Airport* (E.D. Mich. 2012): Court held that a "request for the entire Facebook account, which may well contain voluminous personal materials having nothing to do with this case, is overly broad."
    f. *Flores v. Saravia* (N.Y. Sup. Ct. 2013): Court denied party's request for an order compelling defendant to provide certain social media information because the party had no knowledge that the defendant even used social media platforms containing relevant information.
        i. The party showed that it did not even know what social media evidence it was fishing for by making a conditional demand for such evidence: *If* defendant was not a registered user of social media platforms, the party sought a statement under oath confirming the same.
    g. *Zimmerman v. Weis Mkts., Inc.* (Pa. D. & C. 2011): Court granted defendant's motion to compel discovery of the private portions of plaintiff's social media profiles because defendant made a threshold showing that the public portions of those profiles contained relevant information.
        i. If a party can show that the public portions of a user's social media account contains relevant information, court will be more likely to accept the argument that discovery of the private portions of the same account might reveal additional relevant information.
3. However, not all courts have required a threshold showing of relevancy before affording a party access to the other party's social media content.
    a. *Giacchetto v. Patchogue-Medford Union Free Sch. Dist.* (E.D.N.Y. 2013): Court ordered limited discovery of portions of plaintiff's social networking postings, pointing out that

the Federal Rules of Civil Procedure do not require a party to prove the existence of relevant material before requesting it.

b. *Holter v. Wells Fargo & Co.* (D. Minn. 2011): Holding that defendant was entitled to discovery of plaintiff's social media postings because plaintiff claimed emotion distress, regardless of any threshold showing of likely relevance.

4. A party serving written discovery requests should update its definition of "document" to include social media content, including profiles, postings, walls, pictures, videos, messages, chats, etc.

5. If the party refuses to respond to a request for production, execute a subpoena and seek a court order directing the party to execute a consent that would satisfy the SCA.

   a. *Al Noaimi v. Zaid* (D. Kan. 2012): Finding that because an individual was a plaintiff in the case, the court had authority under Rules 26(b)(2) and 26(c) to order him to execute a consent that would satisfy the SCA.

      i. Defendant could then subpoena social media provider, including with subpoena plaintiff's authorized user consent to disclosure of the information in question.

      ii. Although, as explained above, the exceptions to the SCA's prohibitions (including user consent) only means that covered provider may voluntarily disclose content information, this is the best approach, as a subpoena to a social media provider standing alone does not authorize the provider to disclose the information.

   b. If successful in getting the court to compel the party to sign the consent, send the court order and executed authorization to the social media provider.

   c. Best practice: Once the valid authorization has been sent (thereby getting around the social media provider's likely SCA objection), instruct the provider to send the content to you directly and in native format.

      i. But keep in mind that court will not be able to *compel* social media provider to respond to civil subpoena.

   d. However, getting a court to order a party to execute a valid authorization is the easy part. Under the SCA, social media providers may produce content pursuant to validly-executed user consent, but they cannot be compelled by the court to do so. *See supra*. This puts litigant in less-than-ideal situation of being subject to the whims of a social media provider.

6. Requests for admission may be useful to confirm that identity of an account or the author of a particular post.

C. Serve a discovery request demanding the opposing party's login information and passwords for all social media accounts.

1. Courts have taken inconsistent approaches when faced with the question of whether such a sweeping discovery request – as opposed to tailored discovery requests – is permissible.

   a. *Romano v. Steelcase, Inc.* (N.Y. Sup. Ct. 2010): Requiring defendant to show that need for access to plaintiff's Facebook and MySpace accounts outweighed privacy concerns raised by plaintiff before compelling plaintiff to provide access to such information.

   b. *Largent v. Reed* (Pa. Ct. Com. Pl. 2011): Granting motion to compel plaintiff's Facebook login information.

i. Court: This is actually the least burdensome method for conducting discovery of social media content because the account holder can still access her account while the opposing party investigates.

ii. However, the court permitted the defendant only twenty-one days in which to inspect plaintiff's Facebook account, after which the plaintiff was allowed to reset her password.

c. *Trail v. Lesko* (Pa. C.C.P. 2012): Court held that a blanket request for login information is *per se* unreasonable because complete access to social media account would allow the adversary access to a great deal of information that has nothing to do with the litigation.

d. *Chauvin v. State Farm Mut. Auto. Ins. Co.* (E.D. Mich. 2011): Court affirmed an award of sanctions against defendant due to defendant's motion to compel production of plaintiff's Facebook password.

i. According to the court, the password request was "intrusive," "annoying," and speculative.

ii. Court surmised that the only purpose for such a broad discovery request was to intimidate and harass.

D. In camera review by the court, after which the court can make its own determinations as to the relevance of the social media content in question.

1. *Offenback v. L.M. Bowman, Inc.* (M.D. Pa. 2011): Judge ordered plaintiff to provide court with his log-in information for his Facebook and MySpace accounts.

2. *Douglas v. Riverwalk Grill, LLC* (E.D. Mich. 2012): Court reviewed "literally thousands of entries" on plaintiff's social media account and then identified the specific entries which it deemed relevant and discoverable.

3. To carry out an in camera review, some courts have even "friended" the parties whose social media content is sought.

a. *Barnes v. CUS Nashville, LLC* (M.D. Tenn. 2010): Judge asked party from whom discovery was sought to "friend" him on Facebook so he could disseminate the relevant information to the parties.

b. Attorneys should exercise caution, however, when it comes to friending opposing parties or witnesses in an effort to conduct their own in camera reviews. *See supra*.

4. While in camera review is an option for discovering social media content, especially if the other parties challenges a social media discovery request, some courts are becoming increasingly resistant to the burdensome task of in camera review.

a. *Tompkins v. Detroit Metro. Airport* (E.D. Mich. 2012): Court declined parties' suggestion that it conduct an in camera review of social media content, stating that in camera review is properly utilized to resolve disputes regarding privilege, not threshold discovery disputes regarding relevance.

b. *Fawcett v. Altieri* (N.Y. Sup. Ct. 2013): Court pointedly refused to engage in an in camera review of social media content when the party seeking such discovery had not shown any basis for making the request or likelihood that relevant information would even be uncovered as a result of the court's efforts.

i. "Courts do not have the time or resources to be the researchers for advocates seeking some tidbit of information that may be relevant."

E. Conduct an attorneys' eyes only review.

1. However, an attorneys' eyes only protective order places serious limitations on a lawyer's ability to fully and frankly advise her client.

VII. THE DUTY TO PRESERVE SOCIAL MEDIA EVIDENCE

A. Data residing on social media platforms is subject to the same duty to preserve other types of electronically stored information ("ESI").

1. Fed. R. Civ. P. 34, which addresses the production of ESI, does not explicitly refer to social media.

a. In fact, the federal e-discovery rules were primarily designed to deal with e-mail and electronic information stored on computers.

b. However, the 2006 notes of the Advisory Committee regarding the amendment of Rule 34 instructs that the term ESI is to be read expansively to include all current as well as future electronic storage mediums.

2. Preservation duty is triggered when a party reasonably foresees that evidence might be relevant to issues in pending or foreseeable litigation.

3. Even though a party may not ultimately have to produce its ESI, it still must take appropriate steps to ensure that all potentially relevant ESI is preserved once litigation is pending or foreseeable.

B. Duty to preserve extends to all evidence in a party's possession, custody, or control.

1. Courts construe "control" broadly to include data which a party has a legal right to obtain or a practical ability to access.

2. A party has a right to access its social media content.

a. However, since social media accounts are maintained in the cloud, it might be difficult or impossible for an individual user to access certain metadata associated with his or her profile.

i. For example, if a photo posted to a social media profile is important to a case, it might be necessary to determine who took the photo.

ii. Forensic analysis can reveal metadata in the file that might show details such as when the photo was taken and on what make and model of camera.

3. At a minimum, a court will consider whether a party has made a good-faith effort to comply with its obligations to preserve relevant ESI information.

C. Facebook and Twitter have tools specifically designed to preserve social media content, and parties to litigation can use these tools to satisfy preservation and discovery requirements.

1. Facebook's Download Your Information ("DYI") tool.

a. Accessible to all Facebook users through Facebook's Settings.

b. Allows a user to download a zip file containing personal account data, including timeline information, posts, messages, and photos.

c. DYI is a useful tool in the context of civil litigation because the download contains more information than what is available simply by logging into a user's account, including the ads a user has clicked on and information regarding IP addresses used to log into or out of Facebook.

2. Twitter Archive.

    a. Allows users to download a complete index of every tweet they ever sent from their profile.

D. Other social media providers do not provide such preservation tools.

1. As an example, Instagram explicitly states that it will only make active efforts to preserve data for law enforcement efforts, and even then "[p]reservation requests must include the username of the Instagram account in question, a valid return email address, and must be signed and sent on law enforcement letterhead."

E. Although these "self-help" methods provide a start for preserving social media content, they do not capture all possible data.

1. What about flash content?

    a. Flash content, including Adobe Flash content, refers to the graphic animation used on web sites to make the interactive.

        i. Used widely by social media sites.

    b. May be impossible for a party to litigation to effectively capture constantly-changing flash content without engaging outside service providers.

        i. There is web crawling software available that takes daily snapshots of websites, but at a cost.[10]

2. If an individual user has deactivated his or her account/profile, whether content information has been preserved (and thus can be accessed) will depend on the individual policy of the social media provider…which in most cases will not be that helpful to a litigant. Furthermore, even if the social media provider can and will grant access to a deactivated account, what content information is left will likely depend on whether the user deleted or preserved information prior to deactivating.

    a. Facebook has a policy that states: "If a person cannot access their content, Facebook may, to the extent possible, attempt to restore access to a deactivated account to allow the person to collect and produce content, however Facebook cannot restore account content deleted by that person. Facebook preserves account content only in response to a valid law enforcement request."

F. Don't forget about the metadata!

1. Metadata is essentially "information about information."

    a. Metadata provides important substantive information that could be useful in litigation.

2. In the case of social media evidence, metadata includes:

    a. Dates of creation or access;

    b. The user's IP address;

    c. What smartphone or device was used to create a social media post;

    d. Authors;

    e. Prior history;

[10] National Archives & Records Administration, *Best Practices for the Capture of Social Media Records*, http://www.archives.gov/records-mgmt/resources/socialmediacapture.pdf (May 2013) (last visited Apr. 22, 2014).

f. Editing history; and

g. Management and retrieval information.

3. To be as complete, preservation of social media evidence should include preservation of metadata. Preserving metadata is also helpful for authentication purposes.

   a. Simply taking a "screen shot" of a user's social media page will not capture important metadata.

   b. Facebook's DYI was not designed with litigation or the rules of e-discovery in mind, and it misses comments and metadata fields necessary for complete discovery.

4. Unfortunately, the average lay person does not have the knowledge or technology necessary to capture every piece of metadata. If preservation of metadata is identified by a litigant as being necessary to authentication or some other aspect of the case, the party should consider hiring a computer forensics professional.

   a. As social media usage continues to rise, so too does the number of companies that specialize in the preservation of online content for use in litigation.

   b. Most of these companies emphasize their "crawling" technologies, which allow them to capture social media content in its native format, as opposed to relying on screen captures that do not reveal any metadata.

G. Severe sanctions can result from a party's failure to preserve social media evidence.

1. *Allied Concrete Co. v. Lester* (Va. 2013): Lawyer told paralegal to make sure client "cleaned up" his Facebook page. Paralegal proceeded to help client deactivate his page and delete 16 pictures from account.

   a. Pictures were recovered by forensic experts, but court imposed sanctions on the lawyer ($542,000) and his client ($180,000).

   b. Lawyer also faced disciplinary hearing regarding his role in the Facebook "clean up" efforts.

2. *Gatto v. United Airlines, Inc.* (D.N.J. 2013): Plaintiff attempted to deactivate – but instead unintentionally deleted – his Facebook account.

   a. Court issued adverse inference instruction as a sanction for plaintiff's failure to preserve relevant evidence.

3. *Katiroll Co., Inc. v. Kati Roll & Platters, Inc.* (D.N.J. 2011): Court held that a spoliation inference was not appropriate, and that sanctions were not warranted, where a party changed his social media profile picture during the course of litigation because he had not been explicitly told to preserve such evidence.

   a. The court found that it was not readily apparent to the party that changing his profile picture would compromise discoverable evidence.

4. Retention policies must be well-documented to avoid the possible inference that any loss of social media content was the result of bad faith.

VIII. THE PRESERVATION LETTER IN THE CONTEXT OF SOCIAL MEDIA EVIDENCE

A. Once a duty to preserve is triggered, courts require parties to issue written litigation hold notices, known as preservation letters, instructing that all data relevant to the pending or reasonably foreseeable litigation must be preserved.

B. Social media content should be specifically mentioned in a preservation letter.

1. Although the same duty to preserve applies to social media as to other ESI, social media data is routinely altered or deleted altogether, so it deserves special attention in the preservation letter.
2. *Katiroll Co., Inc. v. Kati Roll & Platters, Inc.* (D.N.J. 2011): Defendant technically committed spoliation by changing his Facebook profile picture during the course of litigation.
    a. Defendant's original profile picture was evidence of the alleged trade infringement and thus should have been preserved.
    b. Court ordered defendant to restore original profile picture but did not award sanctions to plaintiff because plaintiff had not specifically requested that defendant preserve his Facebook account or otherwise make clear to defendant that changing his Facebook profile picture would constitute destruction of evidence.
3. Best practice: Not only should it specifically mention social media content, but a preservation letter should specifically instruct the recipient to utilize Facebook's DYI or Twitter's Archive to download personal account data and content as soon as possible.

C. Who should receive the preservation letter regarding social media?
    1. All parties involved in the pending or foreseeable litigation.
    2. Possibly certain non-party, social media users whose accounts may contain relevant data, including interaction with one of the parties.
    3. What about the social media provider?
        a. Given the fact that social media content is fluid and users can easily delete previous posts or activities, it might be tempting to send a preservation letter to social media providers themselves.
        b. At least in the case of Facebook, this is probably a fruitless effort.
            i. Facebook will only preserve user content in response to a valid law enforcement request.
            ii. The only bone Facebook throws to civil litigants? If a user disables or deletes his account, Facebook states that it will "to the extent possible, restore access to allow the user to collect and produce the account's contents." *See* http://www.facebook.com/help/133221086752707/.
                (a) However, information from a deleted account is only preserved and available using the DYI tool for ninety days after the deletion.

IX. DISCLOSURE OF SOCIAL MEDIA CONTENT

A. Fed. R. Civ. P. 26(a)(1)(A)(ii) requires that a party disclose a description of all ESI in its possession or control that it may use to support its claims or defenses.

B. Any relevant social media content that a party might want to use thus must be identified in its initial disclosures at the outset of discovery.

C. The disclosure must include disclosure of any metadata that the party may use to authenticate other content.

X. STRATEGIES FOR USING SOCIAL MEDIA EVIDENCE IN TRIAL

Federal Rule of Evidence 1001 defines the following types of evidence:

(a) A "writing" consists of letters, words, numbers, or their equivalent set down in any form.

(b) A "recording" consists of letters, words, numbers, or their equivalent recorded in any manner.

(c) A "photograph" means a photographic image or its equivalent stored in any form.

Given the wealth of information that can be added to websites, social media evidence can take many forms, including video and audio recordings. Although in some instances more detailed metadata may be required to overcome authentication disputes, social media evidence is most often admitted through printouts or screenshots. Such formats are treated as writings under evidentiary rules and generally raise the same basic evidentiary issues presented by other kinds of writings, in particular authentication, hearsay, and the original writing rule. See *Lorraine v. Markel Amer. Ins. Co*., 241 F.R.D. 534, 538 (D. Md. 2007).[11]

A. Authentication

Like other writings, printouts and other writings derived from social media must be authenticated before they can be received into evidence. Under the Federal Rules of Evidence (and similar state rules), authentication of a writing requires the proponent "to produce evidence sufficient to support a finding that the writing is what the proponent claims it is." Fed. R. Evid. 901. Examples of evidence commonly used to authenticate social media evidence include the testimony of a witness with personal knowledge of the writing, comparison of the writing with another authenticated document, distinctive characteristics of the writing, and "evidence describing a process or system and showing that it produces an accurate result." See Fed. R. Evid. 901(b)(1),(3),(4),(9); Paul W. Grimm, et al., *Authentication of Social Media Evidence*, 36 Am. J. Trial. Advoc. 433, 464 (2013).[12]

Though purporting to apply the same test of admissibility, different courts looking at the question of authenticating social media evidence have "unfortunately arrive[d] at widely disparate outcomes," resulting in case law that Judge Grimm calls "clear as mud." Grimm, *supra*, at 441. The cases generally fall into two camps. The first, concerned with the ease by which online identities can be falsified, demands that the proponent lay a detailed foundation to establish the author of the content, setting an arguably "unnecessarily high bar … by not admitting the exhibit unless the court definitively determines that the evidence is authentic." *Id.* "[T]he possibility that the evidence may have been created by someone other than its putative creator – even in the absence of any evidence that in fact this happened – appears to have been sufficient for these courts to exclude the evidence." *Id.* at 455. The second, "better reasoned" line of cases does not apply heightened scrutiny to social media evidence and instead requires only a foundational showing that a reasonable juror could conclude the proffered writing is authentic. *Id.* at 456. Given the current split in authority, however, advocates must be aware of the controlling precedents for and expectations of their particular courts.

1. Insufficient Authentication: *Griffin v. State*

The more stringent line of cases is exemplified by *Griffin v. State*, 19 A.3d 415 (Md. 2011).[13] There, the prosecutor introduced printouts from a MySpace profile to show that the petitioner's girlfriend, Jessica Barber, had threatened another witness. *Id*. at 418. The printouts included a photograph that appeared to be petitioner and Barber together, her birthday, her hometown, and statements containing

[11] The wealth of information available on social media sites may also require redaction of printouts submitted to avoid including unduly prejudicial information. See *Griffin v. State*, 19 A.3d 415, 419 (Md. 2011).

[12] Magistrate Judge Grimm, "a recognized authority on evidentiary issues concerning electronic evidence," also authored *Lorraine v. Markel Amer. Ins. Co*., 241 F.R.D. 534 (D. Md. 2007), a frequently cited case that is "[w]idely regarded as the watershed opinion with respect to the admissibility of various forms of electronically stored and/or transmitted information." *Griffin*, 19 A.3d at 422; *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012).

[13] See also Grimm, *supra*, at 441-48 (citing, *inter alia*, *Commonwealth v. Wallick*, No. CP-67-CR-5884-2010 (Pa. Ct. Com. Pl. Oct. 2011); *People v. Beckley*, 185 Cal. App. 4th 509 (2010); *State v Eleck*, 23 A3d 818 (Conn. App. Ct. 2011)). More recently, Mississippi's Supreme Court also concluded that "[t]he ease with which defendants and alleged victims alike could fabricate a social media account to corroborate a story necessitates more than a simple name and photograph to sufficiently link the communication to the purported author…." *Smith v. State*, 2014 Miss. LEXIS 209, at *21 (Miss. Apr. 17, 2014) (finding Facebook entries inadequately authenticated).

petitioner's nickname. The prosecutor sought to authenticate the profile as belonging to Barber through the testimony of the lead investigator, which the parties stipulated would be that he went to the MySpace website, downloaded a posting, and recognized Barber's photograph. *Id*. at 419. The trial court admitted the printout, but the state's high court reversed.

The Court noted that "anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password." *Id.* at 421. Citing *Lorraine*, the Court also noted that "electronically stored information, with its potential for manipulation requires greater scrutiny … than letters or other paper records, to bolster reliability." *Id*. at 423. The court concluded that Barber's photo, birthdate, and location "were not sufficient 'distinctive characteristics'" to authenticate the printout, "given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the 'snitches get snitches' comment." *Id.* at 424. The court cited other decisions reaching similar conclusions, including *Commonwealth v. Williams*, 926 N.E.2d 1162, 1172-72 (Mass. 2010) ("Although it appears that the sender of the messages was using Williams' MySpace Web 'page,' there is no testimony … regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc….. [T]he foundational testimony … did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page."), and *People v. Lenihan*, 911 N.Y.S. 2d 588 (N.Y. Sup. Ct. 2010) (proponent could not adequately authenticate photos printed from MySpace in light of ability to edit photos). The court noted social media printouts might be authenticated through the testimony of the purported creator of the profile, a search of the purported creator's computer for evidence the computer was used to originate the profile or posting at issue, or "to obtain information directly from the social networking website that links the establishment of the profile to the person who alleged created it and also links the posting sought to be introduced to the person who initiated it. *Id*. at 427 (citing *People v. Clevenstine*, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009), in which, inter alia, "a legal compliance officer for MySpace explained at trial that 'the messages … had been exchanged by users of accounts crated by [Clevenstine] and the victims'").

Two judges dissented, finding that a reasonable juror could conclude based on the photo, birthdate, description of the creator and references to defendant's nickname that Barber had posted the information. *Id*. at 429. According to the dissent, "technological heebie-jeebies" go to the weight of the evidence given by the trier of fact, not to admissibility. *Id.* at 430.

2. Sufficient Authentication: *Parker v. State* and *Tienda v. State*

In contrast, other cases have established a "lower hurdle" for admissibility of social media evidence, concluding that "it is for the jury – not the trial judge – to resolve issues of fact" regarding such evidence. *Parker v. State*, 85 A.3d 682, 683 (Del. 2014).[14] In *Parker*, the prosecutor introduced entries originating from the defendant's Facebook account that contained comments that tended to rebut her self-defense argument. *Id*. The admitted printouts included the defendant's photo, name, and a time stamp for each entry. *Id.* at 683-84. The prosecutor authenticated the entries through the testimony of the victim, who had seen the posts, and distinctive characteristics of the posts themselves. The Delaware Supreme Court acknowledged "a genuine concern that [social media posts] could be faked or forged," but noted "that the risk of forgery exists with any evidence and the rules provide for the jury to ultimately resolve issues of fact." *Id*. at 685-86. The Court concluded "that social media evidence should be subject to the same authentication requirements … as any other evidence." *Id*. at 687. Noting other cases where correspondence was authenticated based on "distinguishing characteristics" such as the nicknames of the parties involved, references to the crimes at issue, or even the sender's email address alone, the Court affirmed the trial court's admission of the Facebook posts. *Id*. at 688.

Parker cited with approval *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012) which upheld the admission of printouts of MySpace profile pages, including "the names and acount information

[14] See also Grimm, *supra*, at 449-54 (citing cases).

associated with thte profiles, photos posted on the profiles, commets and instant messages linked to the acconts, and two music links posted to the profile pages." *Id.* at 635. In the trial of Ronnie Tienda, Jr., the victim's sister testified how she came across the profiles, and the prosecutor also offered into evidence "subscriber reports" and accompanying affidavits subpoenaed from MySpace. *Id*. The subscriber reports showed that two of the accounts were opened under the name "Ron Mr. T" and the third under the defendant's nickname "Smiley Face," that the account holder purported to live in the defendant's city, and that the accounts were registered to the email addresses "ronnietiendajr@" and smileys_shit@. *Id*. The prosecutor also introduced photos "tagged" to these accounts that appeared to be the defendant and quotes from the accounts mentioning the victim's death, descriptions of the shooting and witnesses, music played at the victim's funeral, and complaints about an electronic monitor, which the defendant had been required to wear while on house arrest. *Id.* A police officer from the gang unit also testified about gangs' use of socia media. *Id.* The defense elicited testimony on cross examination regarding the ease with which MySpace pages could be forged and also argued that the facts referenced in the messages were not known solely by the defendant and that there was no expert testimony linking the IP address listed in the subscriber report to the defendant's computer. *Id.* at 636.

After citing *Lorraine* and reciting various ways to authenticate electronic evidence, *id*. at 639-42, the court concluded that "the internal content of the MySpace postings … was sufficient circumstantial evidence to establish a prima facie case such that a reasonable juror could have found that they were created and maintained by the [defendant]." *Id.* at 642; see also *id*. at 645 (reciting "combination of facts … taken as a whole"). The court acknowledged the "possibility that the [defendant] was the victim of some elaborate and ongoing conspriacy" in which "unknown malefactors somehow stole the [defendant's] numerous self-portrait photographs" and knew other details, but concluded "that is an alternate scenario whose likelihood and weight the jury was entitled to assess…." *Id.* at 645-46; see also *People v. Valdez*, 201 Cal. App. 4th 1429, 1436 (2011) (noting "consistent, mutually reinforcing content" of admitted MySpace page, "with no evidence of incongruous elements to suggest planted or false material" and "nothing suggested [the defendant] had a personal enemy with a motive to implicate [him] in future gang crimes by creating an entire site or individual postings on it.").[15]

3. The Judge as Gatekeeper: Rule 104

As noted above, while Federal Rule of Evidence 901 provides guidance as to what types of evidence can authenticate writings, different courts have reached different conclusions as to the quantum and quality of evidence sufficient to authenticate social media writings. Judge Grimm advises that a more uniform body of law would result from a more careful application of Rule 104, whereby only "clearly inauthentic" evidence would be excluded, so long as the proponent has offered sufficient evidence "for a reasonable jury to conclude that the evidence was created by the putative creator." Grimm, *supra*, at 465.[16] Judge Grimm notes that "[i]n the vast majority of cases," the objecting party only speculates, and offers no facts, "about who, other than the putative creator, 'could' have created the evidence." *Id.* at 457-58. In such instances, the evidence should be admitted, and the jury can determine how much weight to give to the evidence. *Id.* at 458. Even where "the opponent proves facts that also would justify a reasonable jury in reaching the opposition conclusion" – that is, where "there is plausible evidence of both authenticity and inauthenticity" – the trial judge should still admit the writing and instruct the jury to decide whether it sides with the proponent or opponent. *Id*. at 458.

[15] Evidence that the website content is password protected also supports authentication. *Valdez*, 201 Cal.App.4th at 1434, 1436 (citing as "key factor" testimony of investigator that only the person who has created a MySpace profile has the password may upload content).

[16] Federal Rule of Evidence 104 provides in relevant part:

(a) In General. The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.

(b) Relevance That Depends on a Fact. When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.

B. Hearsay

Compared to issues of authentication, hearsay objections to social media evidence appear to have been addressed in a more straightforward fashion and subjected to the traditional analytical queries: (1) Is the evidence a "statement" made by a person? (see Fed. R. Evid. 801(a))?; (2) Is it offered to prove the truth of its contents? (see Fed. R. Evid. 801(c)); (3) Is it excluded from the definition of hearsay? (see Fed. R. Evid. 801(d)(1)); and (4) Is it covered by an exception to the general exclusion of hearsay evidence? (see Fed. R. Evid. 803, 804, 807). Grimm, *supra*, at 562-63. A few examples are offered below.

1. Automatically generated electronic notifications are not statements made by a person

Concerns about the veracity of people who are not under oath or subject to cross examination are not implicated by an "electronically generated record [that] is entirely the product of the functioning of a computerized system or process." See *Lorraine*, 241 F.R.D. at 564. Thus, "there is no 'person' involved in the creation of [such a] record." *Id*. 564-65 (citing cases); see also *People v. Hawkins*, 98 Cal. App. 4th 1428, 1449 (2002) (printouts showing when computer files were accessed not hearsay). Thus, in *Smith v. State*, 2013 Miss. App. LEXIS 318, at *21 (Miss. Ct. App. June 4, 2013), *rev'd other grounds*, 2014 Miss. LEXIS 209 (Miss. Apr. 17, 2014), the court of appeal held that an e-mail notification automatically generated by Facebook was not a statement made by a human and therefore was not excludable as hearsay.

2. Evidence offered for purposes other than the truth of the matter asserted is not excluded by the hearsay rule

Social media evidence often is not offered for the truth of specific statements made in postings but rather for other purposes, such as circumstantial evidence of a relationship. See *Lorraine*, 241 F.R.D. at 565-66 (citing cases regarding emails and websites). Thus, for example, statements on a social media website were properly admitted as "circumstantial evidence of gang involvement" rather than "declarative assertions to be assessed as truthful or untruthful"; for example, but rather circumstantial evidence of gang involvement"; that is, the jury was not determining whether "Valdez and his 'Krew" were truly 'Most Wanted' by the 'Ladiez' in Orange County." *Valdez*, 201 Cal. App. 4th at 1437; *cf. Miles v. Raycom Media, Inc.*, 2010 U.S. Dist. LEXIS 122712, at *5, *9 n.1 (S.D. Miss. Nov. 18, 2010) (Facebook page offered to prove the truth of the matter asserted that the owner of the page was a cameraman constituted inadmissible hearsay).

3. Admissions by party opponents are not hearsay

"Given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party." *Lorraine*, 241 F.R.D. at 568 (citing cases). Thus for example, in *Smith*, 2013 Miss. App. LEXIS 318, at *22-23, the defendant's statements in Facebook messages were considered admissions by a party-opponent. See also *People v. Oyerinde*, 2011 Mich. App. LEXIS 2104, at *26–27 (Mich. Ct. App. Nov. 29, 2011) (unpublished) (same).

4. Social media evidence may fall within exceptions to the hearsay rule

"Similarly, given the ubiquity of communications in electronic media …, it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium." *Lorraine*, 241 F.R.D. at 568-69. As such, they may fall within hearsay exceptions for present sense impressions (see Fed. R. Evid. 803(1)), excited utterances (Fed. R. Evid. 803(2)), and state of mind (Fed. R. Evid. 803(3)). See *Lorraine*, 241 F.R.D. at 569-70 (citing cases). Thus, for example, the court

in *Oyerinde*, 2011 Mich. App. LEXIS 2104, at *26–27, admitted Facebook messages the victim sent to her sister and the defendant under the "state of mind" exception.

C. Original Writing Rule

As noted above, social media evidence is generally presented in the form of printouts. Federal Rule of Evidence 1001(d) specifically allows for this, providing that "[f]or electronically stored information, 'original' means any printout — or other output readable by sight — if it accurately reflects the information." Other formats that have been accepted include cutting and pasting chat room communications into a word processing document. See *Lorraine*, 241 F.R.D. at 578, 579 (citing *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002)). Furthermore, secondary evidence of information on social media sites may be necessary given the "tenuous and ethereal nature of writings posted" on the internet. *Id.* at 580 (quoting *Bidbay.com, Inc. v. Spry*, 2003 Cal. App. Unpubl. LEXIS 2057 (2003)).

XI. ETHICAL CONSIDERATIONS REGARDING ACCESS TO AND COMMUNICATIONS THROUGH SOCIAL MEDIA OUTLETS

In addition to procedural and evidentiary rules, litigators must also consider ethical implications of how they use social media sites. Given the interactivity of such sites, an attorney can not only obtain highly personal information about parties, other witnesses, and jurors but also directly interact with them (and with judges, too). While some social media information is publicly available, users still "may have some expectation of privacy in their posts," depending on the privacy settings of those posts. New York County Lawyers' Association (NYCLA) Ethics Opinion 745.[17] Attorneys should be aware of generally applicable rules in their jurisdiction regarding ethical investigations and communications. An overview of potential applications of such rules to the use of social media is discussed below.

A. Addressing Social Media Evidence as Matter of Professional Competence

Understanding how social media work and using them to advance a client's interests is not just a good idea for lawyers – it may be required to meet ethical standards of competent practice. At least with regard to researching potential jurors, "advances in technology allowing greater access to information" has led one court to instruct attorneys to use reasonable efforts to examine jurors' prior litigation history in the court's online database and raise issues of juror misconduct in voir dire prior to trial. *Johnson v. McCulloch*, 306 S.W.3d 551, 558 (Mo. 2010). The American Bar Association's Ethics Committee has not formally opined on whether Internet research on jurors is required, but has noted that "a lawyer 'should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.'" Formal Opinion 466 n.3 (citing Model Rule 1.1, cmt. 8). See also New Hampshire Bar Association (NHBA) Ethics Committee Advisory Opinion #2012-13/05 (noting lawyers "have a general duty to be aware of social media as a source of 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"); Association of the Bar of the City of New York (ABCNY) Committee on Professional and Judicial Ethics Formal Opinion 2012-2.

B. Counseling Clients to Preserve Evidence

As noted above, people post a lot of information on social media sites – not all of which may be helpful to their legal interests (or the legal interest of institutions or other entities on whose behalf they post). Attorneys may (and in some situations, may need to) advise clients on such issues as using the highest privacy or security settings on their social media pages to prevent opposing counsel from gaining access outside of formal discovery procedures and the legal implications of information in their posts. NYCLA Ethics Opinion 745. However, as discussed above with regard to discovery obligations,

[17] An index of ethics opinions by state, with URL links, is provided in the appendix.

attorneys must still comply with "litigation holds" or any other legal requirements to preserve potential evidence for reasonably foreseeable proceedings and may not proffer knowingly false statements in litigation or allow the client to make such statements. *Id.*

C. Investigation of Represented Parties

Most jurisdictions have ethical rules barring attorneys from ex parte communications with represented parties in litigation. As such, several ethics opinions have advised that lawyers may not send "friend" requests to represented parties. See, e.g., San Diego County Bar Association Legal Ethics Opinion 2011-2 ("A friend request nominally generated by Facebook and not the attorney is at least an indirect ex parte communication …. If the communication to the represented party is motivated by the quest for information about the subject of the representation, the communication with the represented party is about the subject matter of that representation."); Missouri Bar Association Informal Opinion 2009-0003; Oregon Formal Opinion No. 2005-164 ("[W]ritten communications via the Internet are directly analogous to written communications via traditional mail or messenger service…."). However, there is no ethical bar to accessing public portions of social media sites. New York State Bar Association Ethics Opinion 843 ("A lawyer representing a client in pending litigation may access the public pages of another party's social networking site (such as Facebook or MySpace) for the purpose of obtaining possible impeachment material for use in the litigation."); Oregon Formal Opinion No. 2005-164 ("Accessing an adversary's public Web site is no different from reading a magazine article or purchasing a book written by that adversary."); San Diego County Bar Association (SDCBA) Legal Ethics Opinion 2011-2.

D. Communications With Unrepresented Witnesses

Attorneys generally may approach third parties who are not represented by counsel for relevant information about their cases, but they are still constrained by ethical rules prohibiting deceitful misrepresentations. Opinions have split as to how much information attorneys must disclose to third parties from whom they seek such information by "friending" them on social media. The Philadelphia Bar Association opined in an advisory opinion that asking a third person to "friend" a witness to obtain evidence by providing truthful information (*i.e.*, actual names) but not disclosing the affiliation with the attorney or purpose of the friend request is deceptive because it omits and purposefully conceals a highly material fact. The fact that the witness accepts "friends" from anyone who asks does not excuse the deceit. The Committee also distinguished the permissible practice of videotaping a party in public; "[t]he videographer does not have to ask to enter a private area to make the video." The Committee also concluded such a friend request would constitute making a false statement of material fact to a witness. Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02. The San Diego County and New Hampshire Bar Associations concur. SDCBA Legal Ethics Opinion 2011-2 ("[T]the attorney should not send [a friend] request to someone involved in the matter for which he has been retained without disclosing his affiliation and the purpose for the request.... [N]o one – represented or not, party or non-party – should be misled into accepting such a friendship."); NHBA Ethics Committee Advisory Opinion #2012-13/05 (citing authorities).

However, the New York City Bar Association has opined that while "[a] lawyer may not attempt to gain access to a social networking site under false pretenses," an attorney may use his or her real name and profile to send a friend request to an unrepresented person "without also disclosing the reasons for making the request." ABCNY Formal Opinion 2010-2. Similarly, Oregon does not appear to require disclosure of more than the lawyer's true identity as an initial matter, but has opined that if the third party "asks for additional information to identify Lawyer, or if Lawyer has some other reason to believe that the person misunderstands her role, Lawyer must provide the additional information or withdraw the request." Oregon Formal Opinion No. 2013-189.

E. Investigation of Jurors

Legal opinions to date support investigating jurors through publicly available social media information. Indeed, decisions like *Johnson* suggest such searches may be required as part of trial counsel's competent preparation. However, rules forbidding communicating with jurors still apply. Thus, for example, NYCLA Formal Opinion No. 743 permits "passive monitoring of jurors, such as viewing a publicly available blog or Facebook page," "provided that there is no contact or communication with the prospective juror and the lawyer does not seek to 'friend' jurors, subscribe to their Twitter accounts, send tweets to jurors or otherwise contact them." See also ABCNY Committee on Professional Ethics Formal Opinion 2012-2 ("Attorneys may use social media for juror research as long as no communication occurs between the lawyer and the juror as a result of the research.").

While counsel should certainly avoid directly trading messages with or sending "friend" requests to potential or sitting jurors,[18] they should also be aware of the technical operation of some social media sites that may notify an individual that someone else has viewed their information. For example, LinkedIn and Twitter may send automatic notifications. See ABA Formal Opinion 466; ABCNY Formal Opinion 2012-2; NYCLA Formal Opinion No. 743, n. 2. At least two New York opinions have noted that even such unintentional, non-substantive contacts *may* be ethically forbidden. NYCLA Formal Opinion No. 743 ("If a juror becomes aware of an attorney's efforts to see the juror's profiles on websites, the contact may well consist of an impermissible communication, as it might tend to influence the juror's conduct with respect to the trial."); ABCNY Formal Opinion 2012-2 ("The transmission of the information that the attorney viewed the juror's page is a communication that may be attributable to the lawyer, and even such minimal contact raises the specter of the improper influence and/or intimidation that the Rules are intended to prevent.").[19] On the other hand, the ABA Ethics Committee has opined that such automatic notifications are communications with the social media provider, not the attorney, and therefore not improper. ABA Formal Opinion 466 ("This is akin to a neighbor's recognizing a lawyer's car driving down the juror's street and telling the juror that the lawyer had been seen driving down the street."). Nonetheless, it is worth noting that at the very least, as a practical matter jurors may be uncomfortable knowing that counsel is investigating them, although the ABA opines that proper instructions from the trial judge "will dispel any juror misperception that a lawyer is acting improperly merely by viewing what the juror has revealed to all others on the same network." *Id.*

Post-trial, attorneys may contact jurors, including through social media, unless otherwise prohibited by law or court order. ABCNY Formal Opinion 2012-2. Attorneys are still subject to generally applicable rules not to harass or make misrepresentations to the excused jurors. *Id.*

F. Juror Use of Social Media During Trial

At the same time attorneys are investigating jurors, jurors themselves may also be using (or tempted to use) social media during a trial. See e.g., Amy St. Eve, et al., *More from the #Jury Box: the Latest on Juries and Social Media,* 12 Duke L. & Tech. Rev. 64 (2014) (available online at scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1247&context=dltr); Meghan Dunn, *Jurors' Use of Social Media During Trials and Deliberations: A Report to the Judicial Conference Committee on Court Administration and Case Management* (Nov. 22, 2011) (available at http://www.fjc.gov/public/pdf.nsf/lookup/DunnJuror.pdf/$file/DunnJuror.pdf). Threats to the impartiality of a jury can arise in the social media sphere through searching for information about a case, posting comments about the case, friending witnesses, jurors' failure to disclose social media contacts with parties or witnesses, and identifying information about other jurors. St. Eve, *supra*, at 70-76 (citing cases); Dunn, *supra*, at 3-4. Commentators who have surveyed judges and jurors have recommended issuing

[18] "Similarly, an attorney may read any publicly-available postings of the juror but must not sign up to receive new postings as they are generated." ABCNY Formal Opinion 2012-2.

[19] The New York City Bar Association took "no position on whether such an inadvertent communication would in fact" violate ethical rules. ABCNY Formal Opinion 2012-2.

explicit instructions to jurors "early and often" regarding limitations on their use of social media and explaining the need for such restrictions by tying them to general rules necessary for a fair trial. St. Eve, *supra*, at 86-90; Dunn, *supra*, at 6, 8-10. In 2012, the Judicial Conference Committee on Court Administration and Case Management recommended model jury instructions to deter jurors from improper social media use. See www.uscourts.gov/uscourts/News/2012/jury-instructions.pdf. These model instructions have been incorporated into the Federal Judicial Center's Benchbook for U.S. District Court judges as model jury instruction 6.06. See http://www.fjc.gov/public/pdf.nsf/lookup/Benchbook-US-District-Judges-6TH-FJC-MAR-2013-Public.pdf/$file/Benchbook-US-District-Judges-6TH-FJC-MAR-2013-Public.pdf.

Attorneys who discover evidence of juror misconduct through social media use should consult the court rules and ethics opinions of their jurisdiction. See NYCLA Formal Opinion No. 743.

G. Communications With Judges

Litigants and their attorneys should also consider what social media connections they have with the judge before whom they appear. Judges have ethical duties to avoid an appearance of impropriety, and "[a]ll of a judge's social contacts, … including ESM [electronic social media]," are subject to such duties. See ABA Formal Opinion 462. Judges must also avoid ex parte communications concerning pending or impending matters. *Id.* The mere fact that a judge has a social media connection with a litigant does not necessarily require disclosure or recusal, but the judge should consider "the level of social relationship or the perception of a relationship" and "conduct the same analysis that must be made whenever matters before the court involve persons the judge knows or has a connection with professionally or personally." *Id.* "However, nothing requires a judge to search all of the judge's ESM connections if a judge does not have specific knowledge of an ESM connection that rises to the level of an actual or perceived problematic relationship with any individual." *Id.*

Additional Sources

ABA Section of Litigation, 2012 Annual Conference, Apr. 18-20, 2012, *Plunder or Blunder: E-discovery in the Age of Social Media – Mining for Gold and Dodging the Silver Bullet*, *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/13-1_ediscovery_age_of_social_media.authcheckdam.pdf.

ABA Section of Litigation, 2013 ABA Annual Meeting, Aug. 8-12, 2013, *Social Media Evidence – How to Find It and How to Use It*, *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/aba-annual-2013/written_materials/15_1_social_media_evidence.authcheckdam.pdf.

Mallory Allen & Aaron Orheim, *Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them*, 8 WASH. J.L. TECH. & ARTS 137 (2012), *available at* http://digital.law.washington.edu/dspace-law/handle/1773.1/1172.

John G. Browning, *Digging for Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L.R. 465 (2010), *available at* http://heinonline.org/HOL/Page?handle=hein.journals/comlrtj14&div=26&g_sent=1&collection=journals#481.

Margaret DiBianca, *Discovery and Preservation of Social Media Evidence*, AMERICAN BAR ASSOCIATION, http://www.americanbar.org/publications/blt/2014/01/02_dibianca.html (last visited Feb. 28, 2014).

Lindsay S. Feuer, *Who is Poking Around Your Facebook Profile?: The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites*, 40 HOFSTRA L. REV. 473 (2011), *available at* http://www.hofstralawreview.org/wp-content/uploads/2011/12/40-2-Feuer-Hofstra-Law-Review.pdf.

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

James J. O'Keeffe & Joshua C. Johnson, *Social Media and Discovery – New Tools, Same Rules*, 22 J. CIV. LITIG. 523 (Winter 2010-2011), *available at* http://www.gentrylocke.com/files/JCJ-JJO_JournCivLit_Social-Media-Discov.pdf.

Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563 (2011), *available at* http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech563.pdf.

Social Media Ethics Opinions

American Bar Association

ABA Formal Opinion 462 (2/21/13): Judge's Use of Electronic Social Networking Media http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_462.pdf

ABA Formal Opinion 466 (4/24/14): Lawyer Reviewing Jurors' Internet Presence (www.abajournal.com/files/Formal_Opinion_466_FINAL_04_23_14.pdf)

Missouri

Mo. Bar Ass'n, Informal Op. 2009-0003: attorney may not send friend request to opposing party represented by counsel (http://www.mobar.org/ethics/InformalOpinionsSearch.aspx)

New Hampshire Bar Association

Ethics Committee Advisory Opinion #2012-13/05, Social Media Contact with Witnesses in the Course of Litigation, By the NHBA Ethics Committee (June 20, 2013):

http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_05.asp

New York

Association of the Bar of the City of New York (New York City Bar)

Committee on Professional and Judicial Ethics Formal Opinion 2010-2: Obtaining Evidence from Social Networking Websites

http://www.nycbar.org/ethics/ethics-opinions-local/2010-opinions/786-obtaining-evidence-from-social-networking-websites

Committee on Professional Ethics Formal Opinion 2012-2: Jury Research and Social Media

http://www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-formal-opinion-2012-02

New York County Lawyers' Association

NYCLA Committee on Professional Ethics Formal Opinion No. 743 (May 18, 2011): Lawyer investigation of juror internet and social networking postings during conduct of trial. https://www.nycla.org/siteFiles/Publications/Publications1450_0.pdf

NYCLA Ethics Opinion 745 (July 2, 2013): What advice is appropriate to give a client with respect to existing or proposed postings on social media sites [for civil matters]. https://www.nycla.org/siteFiles/Publications/Publications1630_0.pdf

New York State Bar Association

Committee on Professional Ethics Opinion 843 (9/10/2010): Lawyer's access to public pages of another party's social networking site for the purpose of gathering information for client in pending litigation

http://www.nysba.org/CustomTemplates/Content.aspx?id=5162

Oregon

Formal Opinion No. 2005-164: Communicating with Represented Persons: Contact Through Web Sites and the Internet (https://www.osbar.org/_docs/ethics/2005-164.pdf)

Formal Opinion No. 2013-189, Accessing Info rmation about Third Parties

Through a Social Networking Website: https://www.osbar.org/_docs/ethics/2013-189.pdf

Philadelphia Bar Association

Professional Guidance Committee Opinion 2009-02 (March 2009) (regarding asking a third person to "friend" a witness to obtain evidence by providing truthful information but not disclosing affiliation with attorney or purpose of friend request)

www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf

San Diego County Bar Association

Legal Ethics Opinion 2011-2 (Adopted by the San Diego County Bar Legal Ethics Committee May 24, 2011) (regarding attorney "friending" adverse party's high-ranking employees, giving only the attorney's name)

https://www.sdcba.org/index.cfm?pg=LEC2011-2

Date

Social Media User
c/o Social Media User's Attorney
Address

Re: Preservation of Electronically Stored Information, Including Social Media Content, Relating to **Dispute/Claim**.

Dear Social Media User:

Please be advised that our Firm represents Seeking User Content, Inc. with respect to the federal Complaint you filed. I write regarding your obligation under Federal Rules of Civil Procedure 26 and 34, as well as federal common law, to act immediately to preserve all documents, tangible things, and electronically stored information ("ESI") relating to the claims raised in your Complaint.

Our discovery in connection with the above-referenced action will seek ESI, including, but not limited to, e-mails, instant messages and other electronic communications, word processed documents, Internet usage files, and social media content.

The laws and rules prohibiting destruction of evidence apply to ESI in the same manner and to the same extent that they apply to other forms of evidence. Because of its format, ESI is easily deleted, modified, or corrupted. Access to electronic sources of ESI is critical because the paper form of text derived from an electronic file does not preserve the totality of information which is in the electronic file itself, and therefore preservation of the paper text alone does not constitute the full preservation of evidence.

Therefore, demand is made that you take every reasonable measure to preserve all ESI that is potentially relevant to, or likely to lead to the discovery of admissible evidence regarding, the subject matter of this dispute until its final resolution. This includes, but is not limited to, an obligation to discontinue all data destruction that could lead to the modification or destruction of relevant evidence.

Your obligation to take every reasonable measure to preserve relevant ESI extends to any and all social media site content which is under your control. "Social media site" refers to Internet-based social media websites and/or services including, but not limited to, Facbeook, Twitter, LinkedIn, Instagram, Pinterest, Google-plus, Tumblr, YouTube, and FourSquare. You must take all necessary steps to preserve all social media content posted on or transmitted through social media sites, including but not limited to blog entries, wall postings, pictures, videos, messages (private and public), chats, status updates, and comments. You may not, for example, delete pictures, messages, or photos posted by you or others on any social media site. In addition, you may not deactivate or otherwise delete any social media account, as doing so may result in the permanent loss or destruction of relevant ESI.

Until this matter reaches its final resolution, you must maintain an activity log that documents all modifications made to any social media site content that may affect the site's ability to retrieve or process any ESI.

All social media content or other ESI that is relevant to, or likely to lead to the discovery of admissible evidence, regarding the subject matter of this dispute, and which is created subsequent to the delivery of this letter must also be retained. You must instruct all necessary individuals, including any individuals who have access to your social media content, to take whatever steps are appropriate to preserve such evidence.

Sincerely,

SOCIAL MEDIA DISCOVERERS LLP

John Doe

Attorneys for Seeking User Content, Inc.

CONSENT & AUTHORIZATION TO PRODUCE LINKEDIN ACCOUNT INFORMATION

I, the undersigned, am the holder of an account with LinkedIn Corporation ("LinkedIn") in the name set forth below associated with the email address also set forth below ("Account"). I understand that information related to my Account is being sought in connection with the attached subpoena or other process ("Subpoena").

I hereby certify that I am the owner of the Account for which records are requested.

I consent and authorize LinkedIn to produce to the issuer of the Subpoena any and all information related to the Account including but not limited to information about my identity, address, telephone number, alternative email address, my billing information, my online activities, my connections, my postings, my communications and the contents of all other electronic files maintained by LinkedIn related to me and/or my Account.

I have read and understand the contents of the Consent & Authorization to Produce LinkedIn Account Information.

I agree to hold harmless and do forever hold harmless LinkedIn for the disclosure of such information and do forever waive on my behalf, and on behalf of my heirs and assigns, any and all claims resulting from LinkedIn's disclosure of any information related to me or my Account pursuant to this consent.

Section 1542 Waiver. I UNDERSTAND THAT THIS AGREEMENT INCLUDES A RELEASE OF ALL KNOWN AND UNKNOWN CLAIMS. Furthermore, in giving the releases set forth in this Agreement, which include claims which may be unknown to me at present, I acknowledge that I have read and understand Section 1542 of the California Civil Code which reads as follows: **"A general release does not extend to claims which the creditor does not know or suspect to exist in his or her favor at the time of executing the release, which if known by him or her must have materially affected his or her settlement with the debtor."** I hereby expressly waive and relinquish all rights and benefits under that section and any law or legal principle of similar effect in any jurisdiction with respect to my release of claims herein, including but not limited to the release of unknown and unsuspected claims.

Account Holder Name: _____

Email Address Associated with LinkedIn Account:_____

Account Holder Signature:_____ Date:_____

In order for this consent to be effective, the Account holder must (a) sign this certificate, (b) have it notarized as set forth below, and (c) provide the signed and notarized certificate to LinkedIn Corporation; 2029 Stierlin Court; Mountain View, CA 94043, attention: Legal.

ACKNOWLEDGMENT

State of _____

County of _____

On _____ before me, _____

(insert name and title of the officer) personally appeared_____,
who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I declare under PENALTY OF PERJURY under the laws of the State of _____ that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature _____ **(Seal)**

Please send completed, signed and notarized form via certified mail or overnight courier to LinkedIn Corporation, 2029 Stierlin Ct., Mountain View, CA 94043

UNITED STATES DISTRICT COURT
DISTRICT OF SOCIAL MEDIA DISCOVERY

Social Media User,

Plaintiff,

Case No. 12345C

vs.

Seeking User Content, Inc.,

Defendant.

RESPONDENT'S FIRST SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS AND FIRST SET OF INTERROGATORIES

DEFINITIONS

The following definitions shall apply to these requests and interrogatories:

A. "Social media sites" refers to Internet-based social media websites and/or services including, but not limited to, Facbeook, Twitter, LinkedIn, Instagram, Pinterest, Google-plus, Tumblr, YouTube, and FourSquare.

B. The term "document" includes, but is not limited to, information posted on or transmitted through social media sites, including blog entries, wall postings, pictures, videos, messages (private and public), chats, status updates, and comments.

INSTRUCTIONS

A. You may download and print your Facebook data by logging onto your Facebook account, selecting "Account Settings" under the "Account" tab on your homepage, clicking on the "learn more" link beside the "Download Your Information" tab, and following the directions on the "Download Your Information" page.

B. You may download and print your Twitter data by logging onto your Twitter account, selecting "Me" under the "Help Center" tab on your homepage, clicking on "Downloading Your Twitter Archive," and following the directions on the "Downloading Your Twitter Archive" page.

REQUESTS FOR PRODUCTION OF DOCUMENTS

1. Please provide copies of any documents or electronically stored information you have created and/or stored on any social media site regarding your employment with Seeking User Content, Inc.

2. Please provide copies of any documents or electronically stored information you have created and/or stored on any social media site regarding any of the claims or allegations contained in your Complaint.

3. If you have ever created and/or stored any documents on Facebook regarding your employment with Seeking User Content, Inc. and/or any of the claims or allegations contained in your Complaint, please provide a copy of your complete Facebook history, including any and all profile information, postings, pictures, and data available pursuant to Facebook's "Download Your Own Information" feature.

4. If you have ever created and/or stored any documents on Twitter regarding your employment with Seeking User Content, Inc. and/or any of the claims or allegations contained in your Complaint, please provide a copy of your complete Twitter history, including any and all data available pursuant to Twitter's "Archive" feature.

4. Execute and return a consent and authorization form permitting disclosure of all of your social media content and information for each social media site identified in your Answer to Interrogatory Number 1.

INTERROGATORIES

1. Identify every social media site you have used from **date** to the present, including your user name(s), the e-mail address(es) associated with each social media account listed, and the approximate date you joined the website or service.

2. For each of the social media sites identified in your Answer to Interrogatory Number 1, please provide your log-in information, including any username and password.

Dated this **date** day of **month**, 2014.

SOCIAL MEDIA DISCOVERERS LLP

By: _____
Attorney John Doe

Attorneys for Defendant
Seeking User Content, Inc.

000000-1579\14976604.1

The PowerPoint presentation(s) for this session are available at the following link(s):

Amy Schmidt Jones, Margaret L. Wu, and Michael Melendez: #Gotcha!: Litigation Strategies for the Effective and Ethical Use of Social Media Evidence

#GOTCHA! LITIGATION STRATEGIES FOR THE EFFECTIVE AND ETHICAL USE OF SOCIAL MEDIA EVIDENCE

Amy Schmidt Jones, Esq.
Margaret L. Wu, Esq.
Michael Melendez, Esq.

Overview of Today's Presentation

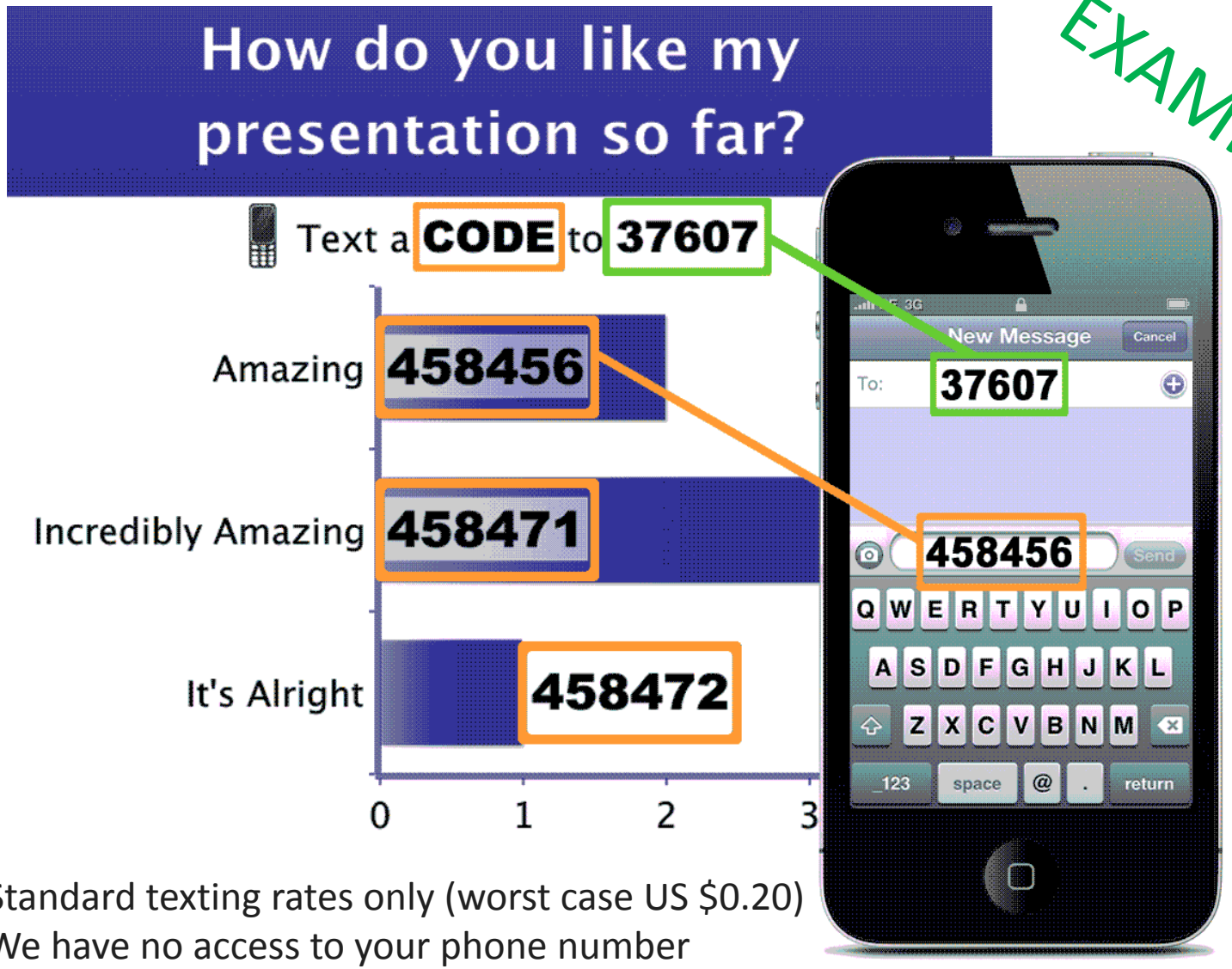
- Brief overview of "social media" and social media usage in higher education.
- The utility of social media evidence in litigation.
- Discovery of social media content.
- The duty to preserve social media content.
- Strategies for using social media evidence in trial.
- Ethical considerations.

What is “Social Media”?

- Interactive, web-based services that allow users to connect with others and share and receive information.
- There are hundreds of social media sites based on every imaginable common interest.

How To Vote via Texting

EXAMPLE



TIPS

1. Standard texting rates only (worst case US $0.20)
2. We have no access to your phone number
3. Capitalization doesn't matter, but spaces and spelling do

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

What Does a Social Media Site Say About its User?

- A lot!
- Creating a social media profile is just like assembling an **"Everything About Me"** folder and sharing the contents with the world.
  - *EEOC v. Orig. Honeybaked Ham Co.* (D. Colo. 2012)

Who is Looking at these "Everything About Me" Folders?

- Perhaps Laura, the diligent, social media-savvy General Counsel of a large university who wonders if she can use social media evidence to assist in pending litigation.

The Utility of Social Media Evidence in Litigation

- Status updates, postings, and photos may establish motive or intent or demonstrate a party's knowledge of particular events.
- Content may contain contradictory statements or other "character evidence."
- Social media content may corroborate key facts.

The Utility of Social Media Evidence in Litigation (cont'd.)

- Identification of potential witnesses.
- Corroborating (or debunking) claims of physical or emotional injuries.
- Determination of current employment status, which may dictate damages.
- Monitor parties' compliance with settlement agreements.

Compliance With Settlement Agreements (Sorry, Dad!)

- Employee sued employer for age discrimination and settled for $80,000.
- Settlement contained confidentiality agreement, which employee's daughter breached when she posted this Facebook message:
  - *"Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT."*

The Discoverability of Social Media Content

- Parties in litigation are entitled to discovery of all relevant, non-privileged information. Social media content is no different.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Why Does Laura Care About Social Media?

- Dr. Overshare was an Assistant Professor at the University. The University received complaints from other faculty members that he was verbally abusive and even harassed some co-workers.
- The University terminated Dr. Overshare after conducting an internal investigation.
- Dr. Overshare denies any wrongdoing and has sued the University for wrongful dismissal.

Will Laura Strike Gold?

- Dr. Overshare is known for sending colleagues lengthy, aggressive e-mails, and he actively maintains several blogs describing his work.
- Laura suspects that Dr. Overshare may have the same tendencies on personal social media sites, and that she might be able to use his social media posts as evidence.
- What might she find?

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Laura Wants to See More!

- Laura notices in Dr. Overshare's public "About Me" section that he lists New College as being his employer since June 2013.
- Laura can also see on Dr. Overshare's "friends" list that he is connected to two of his accusers.
- Laura is happy with the fruits of her Google search but is frustrated that she cannot see more. Other than his "About Me" section and friends list, Dr. Overshare's profile is blocked.

Laura Decides to Go Big

- Laura decides to subpoena Facebook directly and demand that Facebook turn over the contents of Dr. Overshare's profile . . .

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Why Not Subpoena the Social Media Provider?

- Most social media providers will not respond to a civil subpoena for user content.
- The Stored Communications Act ("SCA") provides the legal basis for this refusal.
- Unless a narrow exception is met, the SCA prohibits covered entities from disclosing the contents of users' digital communications, whether voluntarily or under compulsion.

Who is Covered by the SCA?

- Electronic Communication Services ("ECS") and Remote Computing Services ("RCS").
  - ECS: Any service that allows users to send or receive wire or electronic communications, including e-mail and text messages.
  - RCS: Any service that provides users with computer storage services.

Statutory Exceptions to the SCA's Prohibition Against Disclosure

- Disclosure to the government.
- Disclosure of *non-content* information.
  - Very limited exception.
  - Example of non-content social media information may include a user name or a list of the times the user logged into the social media platform.
- Disclosure pursuant to authorized user consent.

Navigating the SCA

- If a party refuses to or cannot comply with discovery request, execute a subpoena and seek a court order directing the party to execute a consent that satisfies the SCA.
- Send executed consent and court order to social media provider.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Caution! Avoiding Ethical Issues

- If you can't do it offline, you can't do it online.
  - No communicating with a represented party.
  - "Friending" is communicating. Accessing publicly available information is not.
- *Piccolo v. Paterson* (Pa. C.C.P. 2011)
  - Court refused to compel plaintiff to accept opposing counsel's friend request.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Avoiding Ethical Issues (cont'd.)

- Asking a third party to "friend" a party or a witness to obtain evidence is deceitful if the third party does not disclose his or her affiliation with the attorney.
- Such a friend request constitutes making a false statement of material fact.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Avoiding Ethical Issues (cont'd.)

- Since Dr. Busybody was not acting as Laura's agent and did not provide the information due to any deception by Laura, she can receive the information and use it in litigation.
  - By posting content on Facebook, Dr. Overshare took the risk that one of his "friends" would reveal the content to the University.

Poll Question

- Dr. Overshare has indicated that his friend, I.M. Inthemix, will corroborate that certain events happened. Laura finds a Facebook page for Mr. Inthemix. Laura believes that Mr. Inthemix's social media posts may be helpful in impeaching his credibility. Laura finds that all of the posts are marked private but sees that he has hundreds of "friends." Mr. Inthemix is not currently represented by counsel.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Serve Well-Tailored Discovery Requests on Individual Party

- Avoid fishing expeditions.
  - Remember Rule 34's "reasonable particularity" requirement and Rule 26's requirement that information sought be relevant or likely to lead to the discovery of admissible evidence.

Serve Requests for Admissions

- Useful to confirm identify of author of social media content.
  - Ask party to admit to his/her use of social media and the identify of all social media platforms used.
  - Ask party to admit to his/her social media "identities" or usernames.

Laura's Carefully Crafted Discovery Requests

- Laura serves a discovery request on Dr. Overshare demanding the production of all Facebook statuses, posts, or content dealing with his claim against the University, including:
  - Posts discussing his current employment; and
  - Communications with his accusers who appear on his friend list.

Laura's Carefully Crafted Discovery Requests (cont'd.)

- Dr. Overshare's attorney objects, but Laura argues that since his "About Me" section contains information about his employer, it is reasonable to believe that he has shared employment info in his private posts, too.
- Since his friend list shows his connection to certain people, it is reasonable to believe Dr. Overshare has communicated with them.

Laura (and the University) Enjoy the Fruits of Discovery Victory

- Because Laura showed that Dr. Overshare's profile likely contained relevant evidence, he was forced to produce the requested content, which included these statuses:

  - "*^%!! you, University . . . I make more at New College anyway!"
  - Watch your back, Dr. Snitch! Good luck getting tenure in this town

The Duty to Preserve Social Media Evidence

- Data residing on social media platforms is subject to the same duty to preserve as other types of electronically stored information ("ESI").
- Duty is triggered when party reasonably foresees that evidence might be relevant to issues in pending or foreseeable litigation.

The Duty to Preserve Social Media Evidence (cont'd.)

- Party must preserve all ESI in its possession, custody, or control.
  - "Control" construed broadly to include data which a party has a legal right to obtain or a practical ability to access.
  - A party has a right to access it social media content.

Social Media and Cloud Computing

- Users can access social media content they create, but keep in mind that they do not actively maintain this content.
- Content is hosted by social media providers and is subject to third party policies and practices.

Don’t Forget About the Metadata!

- “Information about information.”
- With respect to social media content, includes:
  - Dates of creation or access.
  - User’s IP address.
  - Smartphone or device used to create content.
  - Editing history.
- Since social media content is maintained in the cloud, it might be difficult or impossible for an individual user to access certain metadata.

Social Media Preservation Tools

- Facebook's Download Your Information ("DYI")
  - Users can download zip file of personal account data, including posts, messages, and photos.
  - DYI not designed with litigation in mind, though, and it misses metadata fields.
- Twitter Archive
  - Allows users to download complete index of every tweet sent from profile.
  - But not designed for litigation, either.

Preservation Letter

- Issue preservation letter early that explicitly directs preservation of social media content.
  - Explicitly instruct recipient of letter to utilize Facebook's DYI and Twitter Archive.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

The Ethical Tightrope

- While attorneys can (and should) advise clients on smart social media usage, they must also comply with litigation holds and instruct clients to preserve social media evidence once litigation is pending or foreseeable.
- Fine line between savvy advising and required preservation.

Laura Prepares for Trial

- Unfortunately, the University is unable to reach a settlement with Dr. Overshare, and Laura must gear up for a jury trial.
- What must Laura keep in mind if she intends to present the social media content uncovered through discovery as evidence?

The Federal Rules of Evidence and Social Media Content

- Social media content is often introduced through printouts/screenshots, which are treated as writings under the rules of evidence.
- Evidentiary issues include:
  - Authentication.
  - Hearsay.
  - Original writing rule.

Poll Question

- Outside counsel wants to introduce a printout of Dr. Overshare's post in which he talks about his employment with New College.
- In addition to Dr. Overshare's name and photo (the same photo previously used on the Department's website), the Facebook page in question also lists his hometown and has links to articles he has written.

Poll Question (cont'd.)

- Laura can also testify as to how she found the Facebook page through a Google search.
- Dr. Overshare's attorney argues that there is no forensic evidence proving that Dr. Overshare created the page or wrote the post in question.

Your poll will show here

1

Install the app from
pollev.com/app

2

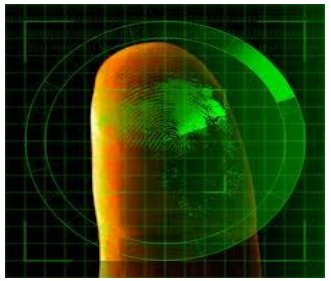
Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Authentication of Social Media Evidence



- Rule 901 requires the proponent "to produce evidence sufficient to support a finding that the writing is what the proponent claims it is."
- Courts fall into two camps with respect to authentication of social media content.
  - Some courts apply heightened scrutiny and require detailed foundation to establish author.
  - Other courts require only that a reasonable juror could conclude that the content is authentic.

Hearsay and Social Media Evidence

- Compared to issues of authentication, hearsay objections to social media evidence have been addressed in a more straightforward, consistent manner by courts.

Additional Ethical Considerations

- Laura and other litigators must consider additional ethical implications of their use of social media content in litigation.

Diligence and Competence

- The competent practice of law requires an awareness of social media as a source of potentially useful information in litigation, as well as how to obtain and use that information.

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Investigation of Jurors

- Attorneys are permitted to investigate jurors through publicly available social media information, but rules forbidding direct communication with jurors still apply.
  - Attorney may not send a friend request to a juror or subscribe to a juror's Twitter feed, for example.

Investigation of Jurors (cont'd.)

- Attorneys conduct informal juror investigation at their own risks.
- LinkedIn, Twitter, and other sites send automatic notifications to users when their content has been viewed.
  - Even such unintentional contact may be ethically forbidden "as it might tend to influence the juror's conduct with respect to the trial."

Jurors' Improper Use of Social Media

- Threats to the impartiality of a jury can arise in the social media sphere through:
  - A juror searching for information about the case;
  - Posting comments about the case;
  - Friending parties or witness;
  - Failing to disclose social media contacts with parties or witnesses; or
  - Identifying information about other jurors.

Warning Jurors Against the Improper Use of Social Media

- Explicit instructions should be given early and often to jurors regarding limitations on their use of social media during the trial.
- Attorneys should monitor for signs of improper social media usage by monitoring publicly available content.

QUESTIONS?