PRESENTING YOUR CASE USING SOCIAL MEDIA: HOW TO PROTECT YOUR CLIENT & YOURSELF FROM ETHICAL PITFALLS

Melissa Fuller Brown[1]
145 King Street, Ste. 405, Charleston, SC 29401
843-722-8900
melissa@melissa-brown.com
www.scdivorcelaw.com

Social media is here to stay. Since almost all our clients are using such media, we are even more challenged in this day and age to fulfill our ethical obligations while also effectively dealing with our client's needs and properly handling and requesting discoverable information.

As of 2014's second quarter, Facebook had more than 1.3 billion active, monthly users. Twitter had 271 million active, monthly users who tweeted an average of 500 million tweets per day. Each month, new forms of social media become available in addition to familiar programs such as YouTube, LinkedIn, Instagram, SnapChat, and What's App.

In the family law arena, social media and the retrieval of electronically stored information (ESI) have become treasure troves of valuable evidence. Since both provide a plethora of information about individuals' habits, communications, photographs, lifestyles, whereabouts, and friends, family court attorneys can search online from the comfort of their office to locate public information on the Internet that was previously costly to obtain through other means. On the other hand, obtaining ESI requires different retrieval methods, and retrieval is often costly as well as the cost to preserve one's own ESI prior to and during litigation.

Technology's usefulness is exciting and time-saving but also time-burdening. It is almost as if the faster and easier we access information and contact others, the more contact we are required to have and the more information we must review. Further, keeping up with technology's rapid advancements is difficult when lawyers are also trying to run their practices and abide by all our other responsibilities. Nevertheless, we cannot live without technology, and in today's world, it impacts almost every single case. Thus, the ABA and some states have added Professional Conduct Rules requirements to specifically address lawyer's responsibility to understand the benefits and risks associated with technology.

The ABA's Model Rules of Professional Conduct, Rule 1.1, places a huge responsibility upon all lawyers, stating "a lawyer… [must] keep abreast of changes in law and its practice, including the benefits and risks associated with relevant technology." In the April 2014 Edition of the *ABA Journal*, U.S. Magistrate James C. Francis of New York was quoted as saying that he sees technological advances like e-discovery as so

[1] Fellow, American & International Academies of Matrimonial Law; Current Chair, AAML Technology Committee; Member, IAML Webinar Committee; Former Chair and current representative, South Carolina Family Law Section.

critical to the courtroom that he views attorneys who are unaware of its nuances as essentially engaging in a slow career suicide. *See* Joe Dysart, *Learn or Lose: Catch Up With Tech, Judges Tell Lawyers*, ABA Journal, April 2014 at 32. Judge Francis also added "E-discovery is pervasive. It's like understanding civil procedure.... You're not going to be a civil litigator without understanding the rules of civil procedure. Similarly, you're no longer going to be able to conduct litigation of any complexity without understanding e-discovery." *See id.*

Literally five minutes before my article's deadline, I received an email from a North Carolina family lawyer familiar with my interest in social media's impact upon our practices. He sent me a proposed ethics opinion (***See* Attached**) that invited North Carolina attorneys to opine about their proposed rules regarding a lawyer's duty to advise clients about social media postings, the propriety of deleting past posts and responsibility to preserve past posts, and the propriety of advising clients to change and or implement security settings on their social media sites.

The proposed opinion seemingly imposes a heavy burden upon lawyers. It almost assumes we should be held to an obligation to anticipate future events or that we always assume every client uses social media or a form of ESI. Another North Carolina education lawyer, Neal Ramee,[2] shared his thoughts about the proposed ethics opinion. He wrote that the rule should address whether a lawyer "**may**" (versus "must") advise clients about the propriety of posting to social media sites. He analogized the situation to his not being "aware of any ethics opinion requiring lawyers to advise their clients of the potential negative effects of any 'existing . . . , future . . . , and third party communications with friends, family, or acquaintances via any of these other modes of communications." However, he suggested that if the North Carolina State Bar believed a lawyer "'**must**' advise clients on social media postings at times, the circumstances should be *limited* to occasions when a lawyer has actual knowledge that a client has posted or intends to post something on social media that is reasonably likely to have a material, adverse impact on the client's legal matter.

Neal Ramee raises an important point especially where most of the published opinions that hold lawyers and clients liable for spoliation or improper handling of ESI are involving millions of dollars with clients who could afford to pay their attorneys, experts and teams of IT people. Those litigants are vastly different from the typical family court litigant who pays his or her legal and expert fees out of their own pocket. The cases that are creating the law typically involve wealthy corporations with deep pockets and expense accounts. The federal cases, however, are the leading cases and likely, there is a future trickle down effect that will impact state court decisions and possibly negatively affect smaller cases if all parties are held to the same standards.

I have struggled with this very issue as the rulings in the federal cases could impose huge, undue burdens upon the typical family court litigant. I am also thrilled that another attorney succinctly addressed his concerns in a manner that makes sense.

[2] Partner, Tharrington Smith, LLP, 150 Fayetteville Street, Suite 1800, Raleigh, North Carolina 27601.

Yes, social media and ESI are here to stay, but we need a reasonableness test or approach when expecting the average individual or business to comply with some of the costly burdens (i.e., Should an individual with an inexpensive computer with limited storage space be obligated to save every piece of spam, junk mail, and frivolous emails in the name of insuring they are preserving all evidence? Who will pay to review all this evidence? How is it reasonable to expect preservation if actual preservation and resulting storage of the preserved ESI make the computer ultimately inoperable?).

Obviously, how lawyers advise their client to handle social media postings and ESI are relevant topics, and ones we must address. They are also topics that most lawyers should understand and be familiar with, including how various social media programs work, what constitutes electronically stored information (ESI), what are the legal methods to obtain ESI and social media posts, how a lawyer authenticates this evidence at trial, and when and how to properly advise clients about preservation of such evidence. Lawyers should also be fully aware and knowledgeable about state and federal laws that impose criminal penalties and civil sanctions upon anyone who violates these laws if the evidence is improperly obtained or handled, whether by the client or attorney.

While we can debate whether the federal rulings should trickle down to family court cases and impracticality of imposing unreasonable financial burdens upon all parties, this article will instead discuss the published opinions and generally advise what this author believes is a wise course of action lawyers should consider to avoid harming their client or themselves. One Virginia personal injury lawyer learned this mistake the hard way. *See Allied Concrete v. Lester,* 285 Va 295, 736 S.E.2d 699 (2013).[3]

No lawyer wants to be the guinea pig example about not properly advising their client. Given technology's rapid rate of change, lawyers and judges alike need assistance to keep up with advances while still managing the business of our daily practices. Thus, the goal of this article is to provide an overview of the current state of the law; to educate attorneys about ESI and other social media; provide tips about how to educate our clients about properly preserving ESI and social media; to inform how to legally obtain and gather ESI from the opposing party and other witnesses; and finally evidentiary rules to lay the foundation to introduce ESI and social into evidence at trial.

[3] In *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013), the lead attorney's paralegal told the attorney that the personal injury client had pictures on his Facebook page that would be detrimental to his case. The attorney told the paralegal to take care of it. Later, it was discovered by Defendant that the Facebook pictures were deleted. (Defendant obtained copies of the photos before Plaintiff deleted them.) The real problem, though, was not the attorney's instruction to his paralegal to "clean up" the problem. The real ethical issue arose when the client, with the attorney's knowledge, denied the pictures ever existed. Both the attorney and client were sanctioned and this ruling was affirmed by the Virginia Supreme Court.

I. Electronically Stored Information (ESI)

ESI is information created, manipulated, stored, and best utilized in digital form.

A. Where is ESI located?

ESI is found on devices with electrical, digital, magnetic, wireless, optical or electromagnetic capabilities such as laptops, iPads, iPhones, iPods, tablets, Android Smartphones, etc.

B. Why is ESI so important to the practice of family law?

Today, people use these various devices to communicate with others through emails, texts, pictures, videos, posts, tweets and the like. As such, these communications are often key evidence in family court cases.

While some may think that ESI is a relatively new phenomenon, it first became relevant on the national horizon during the Iran-Contra affair. In the late 1980's, United States Senate investigators were able to retrieve 758 email messages sent by Ollie North to the Contras. These emails were the smoking gun that confirmed North's involvement in that operation despite his denials to a Senate Committee while under oath. Interestingly, North was convicted but not for his involvement with selling arms to the Contras. Instead, he was convicted for perjury - lying to the Senate Committee about the emails while under oath.

In 1999, the ABA adopted the Civil Discovery Standards that included rules about handling e-discovery. Then, in 2006, the Federal Rules of Civil Procedure formally changed to include language about the use of electronic discovery.

In 2003, Judge Shira A. Scheindlin, a federal judge in New York well known for her knowledge of technology and the use and abuse of e-discovery, cited the civil discovery standards and the scope of a litigant's duty to preserve electronic documents in her seminal decision *Zubalake v. UBS Warburg*, 216 F.R.D. 280, 283 n. 30 (S.D.N.Y. 2003). Now, a majority of states have enacted e-discovery rules, and ESI is an explicit part of the 2006 amendments to the Federal Rules of Civil Procedure.

C. Why do I need to understand ESI?

As the law has evolved to keep up with technology, more judges have held attorneys liable for not properly advising their clients how to preserve ESI. In 2008, Magistrate Barbara Major sanctioned Qualcomm and some of its retained attorneys when Qualcomm destroyed tens of thousands of emails. *Qualcomm v. Broadcomm*, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008).

Ten years after *Zubalaki*, Judge Scheindlin issued a scathing opinion and jury charge and held Plaintiff's attorneys liable for not properly advising their client, Sekisui America Corporation, about how to preserve ESI data and for not ensuring that their client properly complied when responding to an e-discovery request. *Sekisui America Corp. v. Hart*, 945 F.Supp.2d 494 (S.D.N.Y. Aug. 15, 2013). Judge Scheindlin also

granted Defendant's jury instruction request and charged the jury to assume Plaintiff's actions in deleting electronic documents were detrimental to Defendant and that sanctions were appropriate.

D. How do the rulings in *Qualcomm* and *Zubalaki* affect family law attorneys?

Since ESI is prevalent in almost every family court case and likely potential evidence, the safest route about whether to advise a client to preserve the evidence is to assume all potential clients' cases are ones where litigation is likely. Therefore, advise the client to preserve all forms of ESI especially where litigation is imminent, and put your advice in writing in your file. The reasoning is as follows:

- Duty to preserve is clear under the Federal rules and under most state rules now.
- Duty to marshal data avoids sanctions.
- Properly advising clients to preserve their information protects the lawyer and client.

II. How do you properly obtain ESI from the opposing party?

ESI can be obtained in a myriad of ways. Below is a brief discussion outlining methods to legally gather ESI as evidence to introduce in court.

A. How do you properly download evidence from the Internet?

There are several ways to authenticate social media postings, but the safest way is to first create a PDF file of the image so its appearance as it appears on the Internet is preserved. To create the duplicate image, print the page as a PDF. Doing so also includes the page's URL, the Internet address of the page on the Web, and the date the image was viewed.

Our office uses Apple computers, and they are set up to allow you to print a document to PDF. This means that you do not actually "*print*" the document, but the print feature turns the image, web page, photograph etc into a PDF that you save to a file and then print on your printer. Another method is to use Adobe Acrobat Pro (not Adobe Reader) to create a PDF file.

The reason this method is best is that turning the ESI image into a PDF identifies the web address and the date the image was online, which helps authenticate the veracity of the document as being the image that the proponent saw online. The last step is to choose a safe, secure location to save the PDF for future use.

B. What are Litigation Hold, Preservation and Spoliation Warning Letters?

Litigation Hold, Preservation and Spoliation Warning letters are a means to put the other side on notice to preserve and refrain from destroying any ESI evidence that might be related in any way to the litigation.

1. Why are these letters so important?

These letters are important to send early in a case to put the opposing party on notice to preserve all ESI and not to destroy any potential evidence

While Plaintiff was punished in *Sekisui*, Defendant's attorney was slammed in *Green v. McClendon*, 2009 U.S. Dist. LEXIS 71860 (S.D.N.Y. Aug. 13, 2009). In *Green*, the New York judge held that the "litigation hold duty" *first runs to the lawyer* and only then does the duty run to the client. In this case, the court found the lawyer failed to properly instruct the client to preserve relevant evidence in the case and, because the lawyer failed to advise and instruct the client about the preservation of evidence, the court found the lawyer, not the client, liable----scary stuff for family court attorneys.

Craig Ball wrote an article titled, "The Perfect Preservation Letter." This article discusses the features contained in a *perfect* preservation letter, and it offers suggestions about effectively drafting and deploying the proper language that is specific to your case. Ball advises:

> "Outlaw musician David Allan Coe sings of how no country and western song can be "perfect" *unless* it talks of Mama, trains, trucks, prison and getting drunk. Likewise, no digital evidence preservation letter can be "perfect" unless it clearly identifies the materials requiring protection, educates your opponent about preservation options and lays out the consequences of failing to preserve the evidence. *You won't find the perfect preservation letter in any formbook*. You have to build it, custom-crafted from a judicious mix of technical boilerplate and *fact-specific* direction. It compels broad retention while appearing to ask for no more than the bare essentials. It rings with reasonableness. It keeps the focus of e-discovery where it belongs: relevance."

See Craig Ball, "The Perfect Preservation Letter"
http://www.craigball.com/perfect%20preservation%20letter.pdf

2. What entails a showing of good faith?

A showing of good faith has always been necessary when responding to discovery or any other court-ordered instruction; however, the **burden of showing good faith is now significantly greater** on the part of the responding party.

Attorneys cannot claim that they did not know about those backup tapes stored in a closet or have proper access to IT personnel.

Counsel must have proactive conversations with ESI custodians and IT stewards to create and maintain documentation regarding what preservation actions were taken when the obligation arose, how the chain of custody was assured and how both custodians and relevant ESI repositories were systematically identified.

3. Metadata

Even if there are hard copy documents of ESI available, the hard copies do not contain the metadata that is attached to the digital image. Metadata is key information because it is often *where the real gems are hidden*. Metadata are document attributes about the creation, modification, authorship and other potential details based on the application used to create the electronic documents.

Metadata may also be used for admissibility purposes because it can demonstrate the chain of custody for a particular piece of ESI. It can also be used in the preservation and review process by identifying key information and facilitating the culling of duplicate documents.

Handling and processing electronic evidence presents new and unique challenges that are vastly different from working with traditional printed documents. To prevent spoliation, proper methods must be used in the collection and review of electronic documents. Simply opening a file or copying it to another location may actually modify the hidden metadata and destroy it. Since obtaining this evidence is complex and one must document a clear chain of custody, it is best to hire an experienced forensic computer expert to obtain this evidence.

4. Privilege

Technology has changed the way our world conducts business, and it certainly simplifies many tasks but its rapid pace and rate of productivity can also exponentially create the potential for mistakes. On occasion, it is not unusual to inadvertently disclose a privileged document. On these occasions, using **claw back and quick-peek agreements** can help buffer this risk, yet these agreements are still only partially effective.

Be forewarned. If proper steps to maintain privilege are not taken, courts may find a party waived the privilege. As attorneys, properly advise your client about potential errors so the fault does not rest with you.

5. Facebook spoliation cases and contrasting rulings by different state and federal courts:

a. *Examples Where Parties Were Sanctioned for Spoliation of Facebook evidence:*

Gatto v. United Air Lines, Inc., No. 10-CV-1090-ES, 2013 WL 1285285 (D.N.J. March 25, 2013): Plaintiff argued that he did not destroy his Facebook account. He argued that he merely deactivated it. However, the record included additional evidence indicating that Plaintiff did take additional steps to permanently delete his account.

Allied Concrete Co. v. Lester, 736 S.E.2d 699 (Va. 2013): Recall the facts of this case that are discussed in footnote 3 herein.

b. *Cases Where Parties Were Not Sanctioned for Spoliation of Facebook Evidence:*

Hawkins v. College of Charleston, No. 2:12-CV-384 DCN (D.S.C. November 15, 2013): Judge Norton did not sanction Plaintiff, a former College of Charleston student, for deleting some of his Facebook pages because the Court held Plaintiff's actions were not prejudicial to Defendant.

Osburn v. Hagel, 2013 WL 6069013 (MD Ala. Nov. 18, 2013): Court determined sanctions not appropriate where the Facebook account holder normally deleted her conversations and that she acted in the normal course of behavior prior to receiving discovery requests for this information.

C. Traditional Discovery

Traditional discovery requests (such as Interrogatories, Requests for Production, Requests to Admit, and Depositions) can be used to obtain and authenticate social media ESI. Much like your Preservation Letter, these discovery requests should be custom-crafted and fact-specific to your case. Here are some examples:

1. Interrogatories

- Name and Address of every social networking website used by Plaintiff.
- Each and every user name, screen name, IM name, e-mail address or alias used by Plaintiff with each social networking website.
- Every password and login name for each social networking website.
- URL for each social networking website.
- Last time Plaintiff accessed each social networking website.
- Date Plaintiff last changed his security settings on his social media websites.
- Date Plaintiff last changed his privacy settings on his social media websites.

Interrogatory responses can identify the existence of social media or ESI so that the actual social media can be obtained through specific Requests for Production. Further, the key to making a proper RFP request is to ask for the social media or ESI in its native format.

2. Requests for Production

Specifically draft your requests for this information to be provided in its original, native format. Below are sample Requests for Production:

- For each of your social media accounts, produce your account data from and including the date of marriage (November 12, 2011) through present. You may download and print your Facebook and Twitter data by logging onto your Facebook or Twitter 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.
- Provide copies of each page of Plaintiff's social media websites.
- Provide copies of all posts made by Plaintiff on each social media website.
- Provide copies of all posts by others on each of Plaintiff's social networking websites.
- Provide copies of every photograph downloaded/uploaded to each of Plaintiff's social media websites.
- Provide copies of all direct messages sent and received by Plaintiff on each of his social media websites.

3. Examples of Social Media/ESI Requests to Admit

- Defendant maintains a Twitter account.
- Defendant's Twitter user name is @XXX.
- On July 1, 2014, Defendant posted a tweet stating "can't wait to quit my job tomorrow so I can head to the beach early for July 4th!! #Partynonstop."

4. Depositions

Another way to authenticate online evidence is to ask the actual poster to admit to posting the statement or tweet during a deposition prior to trial.

D. Cellebrite Touch

A new device and software created by the Israelis and used by many law enforcement groups and computer forensic experts is Cellebrite Touch. It is a product that creates images of information located on cell phones. A one-year license costs $5,000. Once one is properly trained to use the device, Cellebrite allows the expert to copy a cell phone and create a verifiable copy for later use at court.

It is best for the client, not the attorney, to take the phone to the expert to protect

the chain of custody. The expert will identify and note the information about the phone, serial number, owner, condition of the phone including scratches, and whether it was on or off when delivered, and the expert will photograph the phone.

Cellebrite Touch simply creates images. It does not analyze the actual material. Obtaining the images can take a long time. For example, it takes one hour to download images from a phone with 1Gb of memory. Most phones have at least 16 Gb of memory and many have much more. Thus, it will take Cellebrite 64 hours to download images from an iPhone 5 with 64 Gb of memory.

Cellebrite captures contacts, emails, photographs and calendar entries, although, if contacts and calendar entries are modified, it does not keep a historical track of information.

With emails, the device is able to identify the origin of the source or transmission. Then there is the data extraction. Interestingly, experts can generally get around the passwords on iPhones, but the outdated Blackberries have one major benefit over iPhones and that is that the Blackberries encryption is solid.

Text messages are also extractable, and there will be a timeline that accurately shows the user's activity including time and date for photos and sometimes even the location where the photo was taken.

E. Other Mining for Social Media ESI

Tools such as Z-1 Social Discovery software allows the user to legally "troll" the publically available information on a subject's social media account. This tool and others such as Archive Social collect the data offline as it is being posted and compiles it for later review. There is a question as to whether these tools will capture the Xpire or Cyberdust communications that are intended to disappear when read or after a specified number of seconds.

III. Ethical Concerns in Obtaining ESI

A. Ethics Tips

- Avoid using third parties to contact counsel, parties, or witnesses without expressly disclosing that the communication is on behalf of the attorney, law firm, or client.
- Never use deception or misrepresentation in communications – including use of aliases and screen names that do not clearly identify you.
- Always clearly identify yourself and the purpose of your communications.
- Understand and follow user rules associated with sites.
- Check with your state and local ethics boards for recent decisions to stay updated.
- If it feels wrong, don't do it.

See Tiffany M. Williams, Facebook: Ethics, Traps and Reminders, ABA, Section of Litigation News (August 27, 2009).

B. New York Bar's Social Media Ethics Guidelines

Recently the New York Bar Association's Commercial and Federal Litigation Section issued some ethical guidelines to be considered when obtaining social media as evidence. *See* NYSBA Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York Bar Association at www.nysba.org/Sections/Commercial_Federal_Litigation/Com_Fed_PDFs/Social_Media_Ethics_Guidelines.html. The Introduction to the "Guidelines" state: "as use of social media by…clients continues to grow and as social media networks proliferate and become more technologically advanced, so too do the ethical issues facing lawyers." *Id.*

In the July 25, 2014 Litigation News, Erin Louise Primer discussed the Guidelines and highlighted the following sections:

- "Guideline 3.A allows a lawyer to freely access the public portion of an individual's social media website or profile, regardless of whether that individual is represented by a lawyer."

- "Guideline 3.B allows a lawyer to request to review the restricted portion of an unrepresented individual's social media profile as long as the lawyer does not attempt to shield her identity and as long as the lawyer honestly answers any questions that the unrepresented individual might have."
    - Guideline 3.B "recognizes conflicting guidance in different jurisdictions regarding how much information a lawyer must disclose in requesting to review the restricted portion of an unrepresented individual's social media profile."

- "Guideline 4.A provides that a lawyer may advise a client to remove content as long as it would not violate any decision, statute, rule or regulation on spoliation of evidence. An individual cannot delete content that is subject to a duty to preserve unless an 'appropriate record' of the information is created."

- "Guideline 4.B allows a lawyer to suggest that a client create a new social media content, as long as that content is not false or misleading information that is relevant to a claim." See Erin Louise Primer, New York Bar Issues Social Media Guidelines, Litigation News (July 25, 2014).

- "Under Guideline 4.C, a lawyer cannot use false statements in litigation if the lawyer learns from a client's social media profile that the statements are false."

- "Guideline 4.D allows a lawyer to review information from the restricted portion of a represented individual's social media profile that is provided by the lawyer's client as long as the lawyer does not inappropriately obtain confidential

information about the represented person, invite the represented person to take action without the advice of his or her lawyer, or otherwise overreach with respect to the represented person."

- "[C]omment to Guideline 4.D states that a lawyer can advise a client regarding communications with a represented party where the client conceives the idea to communicate with [the] represented party and the lawyer does not take action without the advise of counsel or otherwise overreach the nonclient."
    - "New York interprets 'overreaching' as prohibiting a lawyer from converting a communication initiated or conceived by the client into a vehicle for the lawyer to communicate directly with the nonclient."

See Erin Louise Primer, New York Bar Issues Social Media Guidelines, Litigation News (July 25, 2014).

C. Relevant federal laws affecting ESI

Part of our duty to explain and educate our clients about preserving ESI is likely the duty to explain how to legally obtain ESI from their spouses. Federal and state laws specifically address this issue so lawyers must educate themselves and their clients so the clients do not violate them. Equally worrisome is the naïve attorney who attempts to introduce the illegally-obtained ESI into evidence as both the client and the attorney could be subject to both criminal and civil penalties.

1. Federal Wiretap Act

"'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data…transmitted in whole or in part by a wire, radio…system that affects interstate or foreign commerce, but does not include…any communication from a tracking device…" *See* 18 U.S.C. § 2510(12)(C)(emphasis added).

2. Stored Communications Act (18 U.S.C. § 2701)

"(a) Offense. — Except as provided in subsection (c) of this section whoever —

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided…" *See* 18 U.S.C. § 2701(a)(1).

In *Jennings v. Jennings*, 401 S.C. 1, 736 S.E.2d 242 (2012), the South Carolina Supreme Court held that it was not a violation of the Stored Communication Act to access another's email account through an account provider and print copies of emails previously read by the recipient. Since, emails are not temporary and not in transmission, the emails residing on respondent's computer were only copies of emails and could not constitute a backup of such communication. Therefore, this practice did not equal the definition of electronic storage.

3. The Computer Fraud Act (18 U.S.C. § 1030)

"(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains —
(A) information contained in a financial record of a financial institution, or a card issuer as defined in section 1602(n)(1) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1601 et. seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer...."

4. Electronic Communications Privacy Act

"Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce...." *See* 18 U.S.C. § 2510(1).

"Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *See* 18 U.S.C. § 2510(2).

IV. Evidentiary Issues in Court

A. Use of Electronic Evidence

Ask yourself whether the evidence is relevant (does the evidence have any tendency to make some fact that is of consequence to the litigation more or less probable that it otherwise would be); is authentic (can the proponent show that the evidence is what it purports to be); if there are any hearsay issues; or if there are any other evidentiary rule concerns.

B. Prerequisites of Admissibility

The admissibility of electronic records is still evolving as most organizations strive to move from paper to paperless records. However, the admissibility of electronic information is more complex and raises issues as to the methodology used in data collection and the chain of custody of the collected electronic data.

Lorraine v. Markel Insurance Company, 241 F.R.D. 534 (D. Md. 2007) is an excellent "primer" that outlines how to admit electronic evidence at trial. To be admissible the electronic evidence needs to be:

1. **Relevant** (Rule 401, FRE): "Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." *See* Rule 401, FRE.

2. **Authentic** (Rule 901(a) - 902, FRE): "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." *See* Rule 901(a), FRE.

    - What was actually on the website?

    - Does the exhibit or testimony accurately reflect it?

    - If so, is it attributable to the owner of the website or social media?

    - "[d]ocuments produced in discovery are presumed authentic." *See* Ian S. Clement, Webpage Held Not Self-Authenticating, Litigation News (July 11, 2014)

        - "[A] proponent could produce an opponent's webpage during Rule 26 disclosures. The opponent's failure to do so waives all objections other than under Rule 402 and 403, unless the court excuses the waiver." *Id.*

        - "[T]he 10 methods of authentication identified in 901(b) [or the list herein] are non-exclusive, as noted by Advisory Committee." *Id.*

    - For example, in *Telewizja Polska USA, Inc. v. Echostar Satellite Corporation*, the U.S. District Court for the Northern District of Illinois permitted the proponent to offer an affidavit from a representative of the Internet Archive Company, which retrieves copies of websites as they appear on certain dates in time through the use of its "wayback machine." *Id.* (citing *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 U.S. Dist. LEXIS 20845 (N.D. Ill. Oct. 14, 2004)).

3. **Not Hearsay** (Rule 801 - 807, FRE): "'Hearsay' means a statement that: (1) the declarant does not make while testifying at the current trial or hearing; and (2) a party offers in evidence to prove the truth of the matter asserted in the statement." *See* Rule 801(c), FRE.

    - Does the evidence constitute a statement, as defined by Rule 801(a)?

    - Was the statement made by a "declarant," as defined by Rule 801(b)?

    - Is the statement being offered to prove the truth of its contents, as provided by 801(c)?

- Is the statement excluded from the definition of hearsay by Rule 801(a)?

- If the statement is hearsay, is it covered by one of the exceptions identified in Rules 803, 804, and 807?

    - Common hearsay exceptions when dealing with social media evidence
        - Present Sense Impression, Rule 803(1), FRE.
        - Excited Utterance, Rule 803(2), FRE.
        - Then Existing Mental, Emotional, or Physical Condition, Rule 803(3), FRE.

4. **Contents of Writings, Recordings, and Photographs**. (Rules 1001 - 1008, FRE):

"An 'original' of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, 'original' means any printout – or other output readable by sight – if it accurately reflects the information. An 'original' of a photograph includes the negative or a print from it." *See* Rule 1001(d), FRE. "An original writing, recording, or photograph is required in order to prove its content unless these rules or federal statute provides otherwise." *See* Rule 1002, FRE.

- If social media data is stored in computer or similar device, any printout or other output readable by sight, shown to reflect the social media data accurately, is an "original."

"A 'duplicate' means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent proves or technique that accurately reproduces the original." *See* Rule 1001(e), FRE. "A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate." *See* Rule 1003, FRE.

5. **Probative Value Must Outweigh the Unfair Prejudice** (Rule 403, FRE):

"The court may exclude relevant evidence if its probative value is substantially outweighed by a danger or one or more of the following: unfair prejudice, confusing the issues, misleading the [fact-finder], undue delay, wasting time, or needlessly presenting cumulative evidence." *See* Rule 403, FRE.

VI. Technology: Presenting Your Case

The best way to present social media evidence or electronic evidence is to use technology. Images of social media content, websites, or emails, make a stronger impact upon the viewer if the images appear as one would normally encounter them in everyday life. Simply, "a [fact-finder] wants to experience evidence in the ways if would experience it in the real world. The best way to present a webpage at trial is to present it

electronically - provided the content of the webpage you are offering has not changed from the time the witness first encountered it to the time of trial. Assuming that is the case, the proponent would go through the same authenticating process." *See* Ian S. Clement, Webpage Held Not Self-Authenticating, Litigation News (July 11, 2014).

My firm uses apps and slideshow presentation software to present electronic evidence in court. We also use witness outlines to ensure the social media evidence or ESI is properly authenticated. In instances where we are only allowed to present testimony and exhibits via affidavits, we ensure that the social media evidence or the ESI is authenticated, and we often submit a short (one page) memorandum of law explaining the evidentiary rule that allows for its admission. Pictures are worth a thousand words, and like pictures, social media evidence is so valuable as to be priceless. Thus, despite the burden of our ethical duty to understand social media and ESI and to educate our clients, there are benefits to having this knowledge that might just outweigh some ethical burdens placed upon us.