Social Media, E-Mail and Digital Evidence—From Discovery to Trial

By Steven N. Peskind[1]

Electronically stored evidence (ESI), consisting of e-mail, text messages, social media posts, and other digital data, factors prominently in all litigation. Technology has unfolded its treasures to trial lawyers: vital evidence is now available in social media posts, online journals and other electronic information. While ESI is not inherently different than any other evidence, it presents unique issues due to its fluidity and intangibility. We need to be aware of our duties, both offensively and defensively with regard to this evidence. This paper will address our ethical obligations as well as tactical and proper ways to use this important information.

1. Duty to preserve evidence:

Litigants have a duty to preserve relevant evidence. As lawyers, we have a duty to advise our clients of this obligation. We must notify our clients not to delete images or posts from social media, unless those posts are not relevant to any aspect of the litigation. Certainly, it is improper and unethical for lawyers to advise our clients to destroy such evidence.

[1] Steven N. Peskind is the Principal of the Peskind Law Firm in St. Charles, Illinois. He is the author of "The Family Law Trial Evidence Handbook" published by the ABA Family Law Section and also serves on the ABA/NITA Family law Trial Institute, presented annually in Boulder Colorado. Mr. Peskind is also a fellow of the American Academy of Matrimonial Lawyers and an elected member of the American Law Institute. He writes and speaks frequently on trial advocacy and evidence.

There is no bright line test when the client's duty attaches. In other words, at what point does the client face sanctions if information is deleted? Once the case has commenced the duty undoubtedly attaches. But some authority exists that it attaches at the point that litigation is reasonably anticipated or that information may be relevant in the event of future litigation. As a general word of caution, when in doubt, insist in writing that the client (or potential client) preserve this information indefinitely.

A tale of caution can be found in the case of *Allied Concrete Co. v. Lester*, 285 Va. 295 (Va. 2013). In *Allied Concrete,* Lester's attorney, through his paralegal, told him to clean up certain unflattering pictures on his Facebook page. He took the pictures off his page. Although the opponent ultimately got the pictures anyway, Lester was sanctioned $180,000 and his attorney was sanctioned $542,000. The attorney later agreed to a five-year suspension for his actions.[2] Generally the intentional spoliation of evidence can be deemed an admission or can warrant dismissal of the action. [3]

Lawyers by nature are rescuers, but we must stop at the point that it steps over the boundary line into unethical conduct. Our clients sometimes act in ways that imperil themselves. But we can't always fix it, and this is an example of an area that requires us to proceed cautiously. After you are retained, send a letter to the client

[2] Debra Cassens Weiss, *Lawyer agrees to five-year suspension for advising client to clean up his Facebook photos,* A.B.A. J., Aug. 7, 2013. Available at http://www.abajournal.com/news/article/lawyer_agrees_to_five-year_suspension_for_advising_client_to_clean_up_his_f

[3] See Walters v Walters 249 P. 3d 214, 218 (Wyo 2011) (it is well settled law that destroying or altering evidence in bad faith gives rise to the presumption that the evidence destroyed would have been unfavorable to the party who destroyed it)

admonishing them not to destroy any evidence, including deleting any social media or other relevant electronic information in his or her possession.

2. Obtaining ESI

As early as possible, notify your opponent in writing of the duty to preserve ESI (or any other information in his or her possession). A letter should be sent with as much specificity as possible to protect your client's opportunity to rely on this potentially helpful information. (See attached form spoliation letter.) If the information is later destroyed or lost, opportunities for sanctions and/or other remedies will be enhanced.[4] This is a vital way to secure necessary information in the possession of your opponent.

3. Discovery of ESI

Use the formal discovery process to obtain ESI. [5] The Illinois Supreme Court discovery rules have not yet been modified to incorporate some of the unique issues related to discovery of ESI. Supreme Court Rule 214 remains the avenue to obtain this information. Depending upon the permissiveness of the judge, request the appropriate passwords in order to personally review the social media information. Otherwise request production of screen shots or printouts of certain information within a relevant time period. Consult with an expert on electronic discovery to

[4] *See Peal v. Lee,* 403 Ill. App. 3d 197 (1st Dist. 2010) (Affirming motion to dismiss with prejudice as appropriate sanction for plaintiff's purposeful spoliation of evidence whereby he discarded hard drives, erased data and otherwise destroyed electronic evidence despite letters from opposing counsel and court's order).

[5] A great resource for information about electronic discovery can be found at http://www.ediscoveryinstitute.org

determine the options for procuring digital evidence. Like in all cases, subpoenas are available to compel information from third parties. But subpoenas raise new issues related to access, compliance, cost etc. [6] Beware of discovery "rabbit holes" and the costs incident thereto. Have a discovery action plan to ensure that limited resources are preserved for necessary information.

Also, you must consider jurisdictional requirements when issuing subpoenas. Third parties outside of the jurisdiction of the court are not required to honor subpoenas. Also, many third parties may not keep the records requested. For example, text messages are frequently unavailable from cell phone providers. Do your investigation regarding the availability of this information before incurring the costs to pursue it.

The general rules of discovery apply to ESI and general fishing trips may be disallowed. Try to refine your specific goals with the requested information to combat motions to deny the discovery requests.[7] As with all discovery, the trial court has the power to monitor and limit discovery requests as too burdensome or tangentially relevant.[8] Use the appropriate discovery rules both defensively as well as offensively to block overly broad or burdensome requests to access your clients ESI. In recognition of some of the unique problems, the Supreme Court has revised its

[6] See "Crafting Subpoenas for Electronic information" by Joseph Kish http://apps.americanbar.org/litigation/committees/technology/articles/110410-subpoenas-electronically-stored-information-rule-45.html

[7] *See Giacchetto v. Patchogue-Medford Union Free Sch. Dist.*, No. CV 11-6323(ADS)(AKT), 2013 WL 2897054 (E.D.N.Y.)(Authorizing defendant to conduct limited discovery of plaintiff's social networking sites.)

[8] "Just as the Court would not give defendant the ability to come into plaintiff's home or peruse her computer to search for possible relevant information, the Court will not allow defendant to review social media content to determine what it deems is relevant." *Holter v. Wells Fargo & Co.*, 281 F.R.D. 340 (D. Minn. 2011)

Case Management Rule 218 (a) to permit the court to conduct an early case management conference to address issues regarding the retention and exchange of ESI. In cases where the opponent's ESI may be a linchpin on your proofs, request such a hearing early in the case to preserve important evidence.

Don't covertly access information from a particular social media site. Lawyers are precluded under the Rules of Professional Conduct from creating a phony friendship to gain access to someone's wall.[9] Also, improper access to information will be raised in cross-examination, and any disreputable behavior may end up inadvertently impeaching your own witness. This is distinguished from your client obtaining proper access, in which case information can be properly copied as necessary.

Computer forensic experts can also be retained to extract ESI from a computer. Obviously the expense involved with this type of procedure can be substantial, but in some instances the benefits may significantly exceed the costs. In the event one wants to examine the computer, request access in a notice to produce so that your forensic expert can copy the hard drive for off-site review. Early in the proceeding, request in writing that the opponent not alter his or her computer hard drive or take any action to jeopardize the information on the computer. As we saw above, such precautions will allow you greater remedies if the information mysteriously disappears.

[9] Steven Seidenberg, *Seduced: For Lawyers, the Appeal of Social Media Is Obvious. It's Also Dangerous,* A.B.A., February 1, 2011.

4. Admission of ESI

All potential evidence (including ESI) must satisfy three criteria: Is the evidence **relevant**? Is the evidence **reliable**? Does the evidence meet the substantive requirements set forth in the **rules** (e.g. hearsay, privilege, original writing rule, etc.)? One must satisfy all three elements in order to admit a particular piece of evidence, electronic or otherwise.

A. Relevance

To be relevant, evidence must be both material and have probative value. Materiality involves the context: does the proposed evidence address a matter that is at issue? Is the evidence germane and helpful for the court's consideration? If not, it is immaterial and thus inadmissible. The potential evidence must also be probative of an issue in controversy. Does the evidence more probably than not help prove a point in controversy? Does it help the judge draw reasonable conclusions? While materiality looks to the evidence in the larger context of the whole case, a piece of evidence has probative value if it is a piece of the puzzle worth considering. ESI, while sometime lurid, may not be relevant to any of the issues in the case.

B. Reliability

Assuming evidence is relevant, it must also be reliable in order for the court to consider it. With regard to tangible evidence, such as documents, photographs or physical objects, establishing reliability is known as authenticating the exhibit. An inauthentic exhibit lacks any probative value. To prove authenticity, the proponent

must preliminarily show that the potential evidence is what it claims to be. This is not a difficult burden but requires a rudimentary showing that the exhibit is legitimate. Ordinarily one establishes authenticity through a witness testifying to the origin of the exhibit, that the item presented is what it claims to be. Exhibits also can be authenticated by admissions or stipulations. Some exhibits are self-authenticating under the rules. If an item qualifies as self-authenticating, it does not need to be authenticated by a witness for admission into evidence.

The general consensus of courts nationwide lessens the burden of proving authenticity: the proponent need only provide some reasonable foundation testimony that the proposed exhibit is what it claims to be.[10] As the Court in *Lorraine v. Markel* observed, "Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation." [11] *Lorraine v. Markel* is probably the most influential decision on the topic of electronic evidence. Many of the basic evidentiary issues concerning electronic evidence are discussed in that opinion. All trial lawyers should read and understand the principles laid out by that court on this thorny topic.

Here is a summary of how to authenticate specific digital information:

I. Faxed documents. While in appearance, a fax appears to be an ordinary writing, it is actually a digital communication. To the extent that it is a writing, the

[10] See, "The Return of 'Voodoo Information': A call to Resist A Heightened Authentication Standard for Evidence Derived from Social Networking Websites". 62 Cath. U. L. Rev. 197 (Fall, 2012)
[11] *Lorrine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D.Md. 2007)

same principles of authentication of any ordinary writing would apply. A writing, like any other exhibit, needs to be authenticated by evidence showing that the writing is what the proponent claims it to be.

If the purpose of the writing is to offer some communication from the author (as opposed to how the document affects the reader), foundational testimony confirming the author of the fax will need to be provided. IRE 901(b)(1) provides that an exhibit can be authenticated by the testimony of a witness with knowledge of its authenticity; the rule is satisfied by "testimony that a matter is what it is claimed to be." Either the author can authenticate the document as his writing, or another witness to its creation could verify its authenticity and veracity. In addition to authentication by a witness, the rules also allow authentication based upon a witness's familiarity with any handwriting on the exhibit.

In addition, in reference to a fax writing, information concerning the procedures and the source of the document need to be provided. The Illinois Supreme Court in *People v. Hagan*[12] set forth the foundation requirements necessary to authenticate a fax document. The foundation should include evidence that the fax documents generally indicate trustworthiness by evidence of their accurateness and the proper use of the machines. Questions need to clarify the process of the fax and identity of the document. Additional questions might include the following topics:

- Information concerning the machine on which it was sent or received;

[12] 145 Ill. 2d 287 (1991)

- Information that the machine was in good working order at the time of the transmittal;
- When it was faxed or received;
- The phone numbers that were entered (if the sender is authenticating);
- Recognition of the printed identifying marks on the document;
- Identification of any machine generated receipts or reports and how they are generated during fax transmittals;
- Confirmation that the exhibit is in the same condition as the time it was faxed.

II. E-mails. As I noted above, the threshold for authenticity is not high. Most commonly, the headers on the e-mails establishing the electronic address of the author suffice to authenticate a particular e-mail. In addition, other collateral information may be used. For example, if the e-mail was a reply to one sent by someone else (with a showing of the e-mail thread), the content of the e-mail and the context could serve as a basis to authenticate it.[13] Establishing foundation via a response or reply to a sender is considered an appropriate means of authentication and the presumption is that the e-mail reply is an authentic response to the earlier communication. IRE 901(b)(4) permits authentication based on the distinctive characteristics of the exhibit including its "appearance, contents, substance, internal patterns, or other distinctive characteristics."

An e-mail could be authenticated either by the sender or the recipient. Also, the court could authenticate the e-mail by comparing it to other e-mails that had

[13] *United States v. Siddiqui*, 235 F. 3d 1318, 1322 (11th Cir. 2000)

previously been admitted. (IRE 901(b)(3)).[14] Some courts have authenticated e-mails based upon the fact that the party opponent produced them during discovery.[15] An expert could authenticate the communication as well, but an expert would only be necessary where a credible claim of fraud is made. If the sender of the e-mail authenticates it, some of the foundational questions would include:

- the electronic address placed on the e-mail is that of the claimed recipient;
- the purpose of the communication (why it was sent);
- if applicable, that the sender received an earlier e-mail and replied to that earlier e-mail;
- the e-mail was actually sent;
- the recipient acknowledged the communication to the sender or took action based upon it.

The other common way of authenticating an e-mail is by offering the testimony of the recipient. The recipient would authenticate an e-mail by:

- Acknowledging that he or she received the e-mail;
- Identifying the electronic address of the sender as being the address indicated on the e-mail;
- Identifying any logos or other identifying information on the e-mail;
- Observing whether the e-mail received was in reply to one sent earlier by the recipient;
- Any conversations with the sender concerning the communication;
- Any actions taken by the sender consistent with the communication.

[14] *See United States v. Safavian*, supra, where the court authenticated an e-mail based upon the header
[15] *Shaghticoke Tribal Nation v. Kempthorne*, 587 F. Supp. 2d 389, 397 (D. Conn. 2008; *John Paul Mitchell Systems v. Quality King Distributors, Inc.*, 106 F. Supp. 2d 462, 472 (S. D. N.Y. 2000))

Often people opposing the admission of an e-mail will cry foul, or make unsubstantiated claims that it was altered or forged. Those unsupported claims are insufficient to claim that the e-mails are unauthenticated. The Court in *United States v. Safavian* confirmed that an opponent of electronic evidence needs to show more to successfully keep a piece of electronic evidence out of evidence:

> The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents). We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world. The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done.[16]

Remember that e-mails, like any other writings, are subject to all of the other evidentiary rules. Even if an e-mail can be authenticated, it must still be subject to an appropriate hearsay exclusion or exception before it can be admitted as an exhibit.

[16] *Safavian*, 435 F. Supp. 2d at 41

III. Text messages and other instant messages. Increasingly, people are using text messages as the their primary form of communication. Authentication of text messages or other instant messaging is not substantially different than any other evidence: the proponent need only establish that the communication is what it claims to be. A Pennsylvania Court reasoned that text messages are really no different than any other type of writing:

> Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa R.E. 901 and Pennsylvania case law . . . We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not

there has been an adequate foundational showing of their relevance and authenticity.[17]

The proponent of the text need not rule out all possibilities inconsistent with authenticity, they only need satisfy the minimal requirement that the document is what it claims to be. Arguments that there was no way of knowing who actually sent the message are insufficient to disqualify the admission of a text message.[18]

Like e-mails, courts have allowed text messages to be authenticated by circumstantial evidence. Text messages have been properly authenticated by screen names, context of the messages and other surrounding circumstances.[19] The Supreme Court of North Dakota addressed the issue of authenticity of text messages at length in *State v. Thompson*.[20] That court reiterated the prevailing principle that authenticity is not a demanding burden and that all uncertainties need not be conclusively addressed before an exhibit is considered authentic.[21] In *Thompson*, the state sought to admit a picture of a text from the defendant to the victim in a domestic violence case. The text was authenticated by the victim testifying about the circumstances between the parties on that day, the knowledge of the defendants phone number and the label ("FR: Jen") on the text message and picture. The court sustained use of the picture of the text despite the fact that no testimony was presented concerning who took the picture and that it was what it purported to be.

[17] *In Re F.P., A Minor*, 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005)
[18] *State v. Thompson*, 777 N.W.2d 617 (N.D. 2010)
[19] *Massimo v. State*, 144 S.W. 3d 210, 215017 (Tex. App. 2004)
[20] 777 N.W. 2d 617 (2010)
[21] *Id.*

The court also allowed testimony about other texts, despite no reproductions or copies of the actual text itself being produced.

In another case, *People v. Chromik*, an Illinois court (relying on *People v. Thompson*) allowed a reproduction of a transcript of a text message that was prepared from an actual text.[22] In Chromik, a high school student who claimed her teacher sexually molested her showed the school's principal lewd text messages purportedly sent from the teacher. The principal typed the messages on his computer. They were printed out, and the student reviewed them for accuracy. The principal reflected the time and date of the text on the transcript, and the victim then signed the transcripts. At the trial, the court permitted use of the transcripts, despite the fact that the spell check feature on the principal's computer automatically changed the spelling from the original text on the transcripts.

Like e-mails, the sender or the recipient of a text can most easily establish their authenticity. If the sender testifies, the foundational testimony to be considered includes:

- The context of the message: why it was sent, its purpose, earlier discussions on a topic of controversy, etc.;
- Knowledge that the number it was sent to was the recipient's;
- Identification of a photograph of the actual text that was sent;
- The process of taking the photograph (who took the photo, what camera was used, that it was an accurate reproduction of the actual text, etc.)

[22] *People v. Chromik*, 946 N.E.2d 1039 (Ill. App. Ct. 2011) (Rule 23 Order)

- Reproduction of a transcript of the actual text, including the procedures of making it (transcript was prepared based upon the actual text, reviewed by the sender and it accurately reflects the actual text);

- Testimony regarding any responsive text received or any verbal acknowledgement by the recipient in relation to the earlier text.

If the recipient testifies, the authentication testimony might include:

- Recognition of the number, digital signature or name of the person he/she received the message from;

- Basis of their knowledge of the sender's number (…that numerous text conversations have been had with this person at that particular phone number in the past);

- The context of the text conversation (earlier texts or discussions on the topic that is the subject of the text);

- If a photo of the text is used, the process of taking the photograph (who took the photo, what camera was used, that it was an accurate reproduction of the actual text etc.);

- Reproduction of a transcript of the actual text, including the procedures of making it (transcript was prepared based upon the actual text, reviewed by the recipient and it accurately reflects the actual text).

IV. Chat Room Communications. Chat room communications are less popular than they once were. People today mostly communicate digitally in other ways; nevertheless, certain chat room communications may be beneficial as evidence in a family law matter. Obviously the easiest way to authenticate the evidence would be to have the sender identify him or herself as the participant in the chat. But where the participant is unavailable to do so, the proponent of the evidence will need to provide circumstantial evidence of the communication. Some of the areas of inquiry may include:

- Knowledge (and the basis of same) of the screen name of the sender of the communication;

- Connecting the content of the chats to admissions or other statements made by the sender;

- The timing of the chats were during a period that the sender was available to engage in the chat (e.g. that they were at home during the period and had a working computer);

- The participant discussed the subject of the chat with a third party who could testify to the conversation.

If a transcript is used, additional foundation questions will be necessary to authenticate it, confirming that the transcript is an accurate reproduction, who prepared the transcript, when was it prepared, etc.

V. Websites and Social Media. More and more, websites, including blogs and social media, are valuable evidence in contested family law matters. Websites such as Facebook and MySpace allow members to make online profiles in individual webpages on which the member can post pictures, videos, and updates about their life and activities. Articles abound in the general media about the impact of Facebook and other social media on family law proceedings.[23] The potentially lurid information available on a person's social media page is an ample resource for family lawyers. The foundational requirements for authenticating a screenshot from Facebook is no different than authenticating a printout from any other website. Principally, the proponent of the evidence must offer foundational testimony that the

[23] Leanne Italie, *Facebook is divorce lawyers' new best friend*, MSNBC.com, June 28, 2010, http://www.msnbc.msn.com/id/37986320. Nadine Brozan, *Divorce Lawyers' New Friend: Social Networks*, N.Y. Times, May 15, 2011, at ST17. Stephanie Chen, *Divorce attorneys catching cheaters on Facebook*, CNN.com, (June 1,2010), http://www.cnn.com/2010/TECH/social.media/06/01/facebook.divorce.lawyers/index.html

exhibit is actually on the website that it is claimed to be, that it accurately depicts what is on the website and that the information is attributable to the owner of the site. [24]

VI. Website authentication

Courts are mixed concerning authentication of webpages. Several courts have held that it is necessary for a website owner to provide the necessary foundation in order to authenticate a page from a website.[25] Other courts have held that printouts from websites may be authenticated by someone who visited the website and printed out information they found there.[26] The more permissive camp allows authentication testimony from the person who viewed and ultimately captured the website image in a printed "screen shot." In order to authenticate the image, the authenticating witness must testify that that the depiction "accurately reflects the content of the website and the image of the page on the computer at which the [screen shot] was made." [27] There are no Illinois cases that speak to this topic.

Those courts relaxing the authentication requirement reflect a more common sense approach to this issue. In an era when the court can access the website on its laptop at the bench and authenticate the screen shot by judicial notice, authentication

---

[24] *Lorrine v. Markel American Ins. Co.*, 241 F.R.D 534 (D.Md. 2007)

[25] See, e.g. *United States v. Jackson*, 208 F. 3d 633, 637; *Novak v. Tucows*, Inc. 2007 U.S. Dist. LEXIS 21269, at *5 (E.D.N.Y. March 26, 2007);*Costa v. Keppel Singmarine Dockyard PTE, Ltd.*, 2003 U.S. Dist. LEXIS 16295, at *9 n.74 (C.D> Cal. April 25, 2003)

[26] See, e.g. *United States v. Standring*, 2006 WL 689116, at *3 (S.D. Ohio March 15, 2006); *Moose Creek, Inc. v. Abercrombie & Fitch Co.*,331 F. Supp. 2d 1214, 1225 n.4 (C.D. Cal 2004) aff'd 114 Fed. Appx. 921 (9th Cir. 2004) (unpublished opinion); *Perfect 10, Inc. v. Cybernet Adventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54

[27] *Toytrackerz LLC v. Koehler*, 2009 WL 2591329, at 6 (D.Kan. Aug. 21, 2009)

by one who captured the screen shot makes sense and conforms with the low threshold for authentication.[28] That being said, the question of authentication is dependent on the circumstances for which the screen shot is offered. And the court's scrutiny of the evidence is somewhat dependent upon the website sought to be accessed. A screenshot from a recognized corporation such as a bank or credit card company would probably concern the court less than a personal blog post or some other site where the content can be easily accessed and manipulated.

Because of the ease of manipulating data, some courts are suspicious of the validity of any website postings:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily…view it largely as one catalyst for rumor, innuendo, and misinformation…Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover the Court holds no illusions that hackers can adulterate the content of any web-site from any location at any time.[29]

But, in general, information posted on a commercial website is considered largely reliable today. In fact, information obtained from government websites has been considered self-authenticated if it can be established that the information is current

[28] *United States EEOC v. E.I. DuPont de Nemours & Co.*, 2004 WL 2347559 (E.D. La. 2004)
[29] *St Clair v. Johnny's Oyster and Shrimp, Inc.*, 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999)

and complete.[30] In light of the relatively loose standards for authentication of evidence found in IRE 104(b) and 901(a), family law courts should allow a visitor to the website to properly authenticate the screen shot – particularly where the evidence is not dispositive of the ultimate issue.

In order to authenticate a screen shot from an ordinary website, the following information should be provided to the court:

- That the witness visited the website;
- When the website was visited;
- Information reflecting that the website had been maintained and was current, as opposed to a stale site that had not been kept current (e.g. postings reflecting current information, dates, etc.);
- How the site was accessed (… e.g. "via Internet Explorer web browser, I did a Google search for the particular website and followed the appropriate links"; or if the address was known, … "I entered the web address into the internet browser and accessed the website directly");
- Description of the website accessed: identifying material on the website including names, addresses, logos, phone numbers, etc.;
- Recognition of the website based upon past visits;
- That the screenshot was printed from the website;
- The date and time that the screenshot was captured;
- That the screenshot in the printout is exactly the same as seen on the compute screen;
- That the printout has not been altered or otherwise changed from the image on the computer.

[30] *United States EEOC v. E.I. DuPont de Nemours*, supra (note 27)

VII. Authenticating Facebook postings and other social media

As mentioned above, a screen shot from a Facebook page or other social media page is a webpage within the social media site at large. Information may be communicated by someone on his/her own page, or as a comment or posting to another's page. Any posting by someone is fair game, assuming it can be authenticated and is otherwise admissible. To authenticate a screen shot from a social media site, additional foundation testimony is necessary. Ordinarily that information will reflect circumstantial evidence concerning the person who posted on the site. For example, information should be provided about the individual page that the information was taken from and how it was accessed. Additional questions could be asked concerning authentication of a posting on a Facebook page. Here are some sample questions to consider:

- Are you familiar with the social media website Facebook?
- How are you familiar with it?
- How long have you been using it?
- Describe generally what you do with the application?
- What is a Facebook friendship?
- How is one created?
- Is Sally Jones your Facebook friend?
- What is a Facebook wall?
- How do you access someone's wall?
- What type of information is found on a Facebook wall?
- Have you ever visited Sally Jones' Facebook wall?

- Did you visit her wall recently?
- On what date?
- What did you see on her wall?
- Did you print a copy of what you saw?
- Here is petitioner's exhibit 12. Can you identify this document?
- Is it an exact copy of what you saw on the screen the day you visited Sally's wall?
- What date did you print it?
- What is the handwriting on this exhibit? (initials of the witness and the date it was printed)
- What does this printout depict?
- Where has this printout been since printing it? (chain of custody)
- Have there been any changes to this document since the day you printed it?

This series of questions assumes the witness obtained access to someone's Facebook information via a prior Facebook friendship. Some, but not all Facebook walls, are accessible to anyone on the web, and the information could be extracted without a prior friendship. Some people, however, require a prior friendship before their information can be accessed.

The Maryland Supreme Court takes a more restrictive approach to authentication of social media sites. In the case of *Griffin v. State of Maryland*, the high court observed, "anyone can create a fictitious account and masquerade under

another person's name or gain access to another's account."[31] The court reflected that a printout from a social media site (MySpace), which is available to all, is different from e-mails and instant messages that are "sent directly from one party to an intended recipient or recipients."[32]

The court held "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication. . . .".[33] In reaching its conclusion, the court suggested three ways to properly authenticate this type of evidence: (1) ask the purported creator if she created the profile and added the post in question; (2) search the computer of the person who allegedly created the profile, examining its hard drive and internal history, to determine if it was that person who originated the profile; or (3) obtain information directly from the social networking website itself that establishes who created and posted the relevant information to the profile.[34] Obviously the procedure recommended by the Maryland high court is more onerous than simply presenting circumstantial evidence verifying the author of a social media post—particularly where the alleged author denies that he/she made the post. However, where the import of the evidence is significant, this approach is a safer way to authenticate social media evidence, rather than simple circumstantial testimony.

[31] *Griffin v. State*, 19 A.3d 415, 421 (Md. 2011).
[32] *Id.* at 427.
[33] *Griffin v. State*, 19 A.3d 415, 424 (Md. 2011).
[34] *Id.* at 427-28.

The same basic principles used to authenticate a screen shot from Facebook would apply to MySpace, LinkedIn, Instagram or Twitter. Remember, the purpose of authentication is to provide the court sufficient proof to believe that the document is what it purports to be. Questions focused on the origination, identification, and purity of the exhibit should be sufficient to authenticate any social media printout. Bottom line: ask enough foundational questions to establish that the exhibit "accurately reflects the content of the Web site and the image of the page on the computer at which the [screen shot] was made."[35]

VIII. Computer generated documents. Documents prepared on a computer, such as word processing documents are authenticated in the same manner as other writings: Is the document offered what the proponent claims it to be? In identifying and authenticating computer-stored documents, additional information may need to be provided to the court to authenticate the record, if its identity or connection to the proceeding is challenged. IRE 901 (b)(9) provides that "**Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result**." This rule would apply to computer-generated documents and it is necessary to reflect the accuracy of their source as part of the foundational testimony. For example, if Sally finds on the home computer a draft of a letter that her husband Bill wrote as a Word document, she would need to establish its authenticity by testifying to the particulars:

- where she found it (what computer);

[35] *United States EEOC v. E.I. DuPont de Nemours*, supra (note 27)

- where on the computer was it found (e.g. in the "My Document" file on the computer);
- the general topic of the writing;
- when she found it;
- when she printed it;
- that the printed copy is identical to the copy she found on the computer;
- that it is in the same condition as when she printed it;
- that the document offered is the same one that she printed off the computer.[36]

While rarely challenged, a spreadsheet prepared with a computer program, such as Excel, may need to be authenticated if the accuracy of the computations is questioned. In that event, additional testimony would need to address the computer equipment used, the version of the software used, the experience of the person with the program, the process followed for the input of data and the accuracy of the computations.

Remember, not unlike other digital evidence, it is not necessary to foreclose all possibilities that the evidence may have been tampered with. The possibility of alterations goes towards the *weigh*t, not the *admissibility* of the evidence. Absent

[36] See *Stafford v. Stafford*, 641 A. 2d 348 (Vt. 1993) (Testimony by a wife that she found a list of husband's extramarital affairs on the family computer was sufficient to authenticate the document)

specific evidence showing that the document was altered, the court should not exclude it.[37]

C. Other substantive rules

Assuming prospective evidence is relevant and reliable, it still must meet the substantive rules of evidence, developed over centuries, to ensure that only proper matters came before a judge or jury for consideration. For example, hearsay rules are designed to ensure that fact finders are not improperly influenced by unreliable out of court statements that are not subject to cross-examination. Privileged information is excluded from evidence as a matter of public policy. While this evidence may be relevant and reliable, certain public policy concerns trump use of the evidence. Also, the original writing rule and the rule of completeness bar otherwise relevant and reliable evidence when credible questions arise requiring the production of an original document. Relevant and reliable evidence must still comport with these rules.

When preparing for trial, consider all potential evidence within the scope of the "Three R's". Make sure the evidence is material, probative, and not cumulative. Confirm the reliability of the evidence. Is the witness testifying from their personal knowledge? Is the testimony based upon proper information rather than speculation or opinion? If exhibits are used, how can you authenticate them? Finally, plan defenses to hearsay or other substantive objections.

---

[37] *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) rev'd on other grounds, 528 F.23d 957 (D.C. Cir. 2008)

5. Conclusion

From an evidentiary perspective, the admission of ESI is no different than the admission of any other evidence. The proponent must establish that evidence is relevant and that it is authentic. Then the proponent must overcome any substantive objections, such as hearsay. But there are unique issues presented with regard to the preservation of and access to electronic information, creating ethical and practical problems unknown before computers became the ubiquitous centers of our lives. Practice wisely: inform your clients of their obligations to preserve important evidence and seek it from the opponent before it is altered or otherwise changed.

Steven N. Peskind
PESKIND LAW FIRM
2445 Dean Street, Suite E
St. Charles, IL 60175-4828
Telephone: (630) 444-0701
E-mail: steven@peskindlaw.com