SUFFOLK ACADEMY OF LAW
The Educational Arm of the Suffolk County Bar Association
560 Wheeler Road, Hauppauge, NY 11788
(631) 234-5588

Electronic Evidence Show and Tell

PRESENTERS

Patrick McCormick, Esq.
Robert A. Cohen, Esq.
Hon. James F. Quinn
Johanna Stewart, Esq.

Program Coordinators: Hon. John J. Leo

May 11, 2016
District Court, Central Islip

Electronic Evidence Show & Tell: Admitting Social Media Evidence

Faculty:

Patrick McCormick, Esq., Campolo, Middleton & McCormick, LLP

Robert A. Cohen, Esq., Tabat, Cohen, Blum & Yovino, PC

Hon. James F. Quinn, Acting Supreme Court Justice, Suffolk County

Program Coordinator and Moderator:

Hon. John J. Leo, Supreme Court Justice, Suffolk County

Suffolk County Bar Association

May 11, 2016

ELECTRONIC EVIDENCE SHOW & TELL: ADMITTING SOCIAL MEDIA EVIDENCE

The seminal case regarding admission of ESI is *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007) (U.S. Magistrate Judge Paul Grimm). The case provides:

> Be careful what you ask for, the saying goes, because you might actually get it. For the last several years there has been seemingly endless discussion of the rules regarding the discovery of electronically stored information ("ESI"). The adoption of a series of amendments to the Federal Rules of Civil Procedure relating to the discovery of ESI in December of 2006 has only heightened, not lessened, this discussion. Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes "such facts as would be admissible in evidence" for use in summary judgment practice. FED.R.CIV.P. 56(e).
>
> This is unfortunate, because considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted. The process is complicated by the fact that ESI comes in multiple evidentiary "flavors," including email, website ESI, internet postings, digital photographs, and computer-generated documents and data files.

I. **COURT RULES**

a. Notice amending § 202.12(b) of the Uniform Rules and Rule 1(b) of Section 202.70(g)

i. Where a case "is reasonably likely to include electronic discovery," counsel must come to court "sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery" and may bring a client representative or outside expert to assist in these discussions.

ii. Prior to the preliminary conference, counsel shall confer with regard to any anticipated electronic discovery issues.

iii. Some considerations for determining whether a case is reasonably likely to include electronic discovery:

1. Does potentially relevant electronically stored information ("ESI") exist?
2. Do any of the parties intend to seek or rely upon ESI?
3. Are there less costly or less burdensome alternatives to secure the necessary information without recourse to discovery of ESI?
4. Are the cost and burden of preserving and producing ESI proportionate to the amount in controversy?
5. What is the likelihood that discovery of ESI will aid in the resolution of the dispute?

iv. NYCRR § 202.12(c)(3)- where the court deems appropriate, it may establish the method and scope of any electronic discovery. In establishing the method and scope of electronic discovery, the court may consider the following non-exhaustive list, including but not limited to: (i) identification of potentially relevant types or categories of ESI and the relevant time frame; (ii) disclosure of the applications and manner in which the ESI is maintained; (iii) identification of potentially relevant sources of ESI and whether the ESI is reasonably accessible; (iv) implementation of a preservation plan for potentially relevant ESI; (v) identification of the individual(s) responsible for preservation of ESI; (vi) the scope, extent, order, and form of production; (vii) identification, redaction, labeling, and logging of privileged or confidential ESI; (viii) claw-back or other provisions for privileged or protected ESI; (ix) the scope or method for searching and reviewing ESI; and (x) the anticipated cost and burden of data recovery and proposed initial allocation of such cost.

II. **EVIDENTIARY HURDLES** – the *Lorraine* decision clarifies that "whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence."

a. **Relevance** – is the ESI **relevant** as determined by FRE 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be)

i. Does the ESI have a tendency to prove or disprove a fact important to the trial?

ii. Rule 401 – required to show that social media evidence has the "tendency to make the existence of a fact...more probable or less probable than it would be without the evidence"

b. **Authenticity** – if relevant under Rule 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be?)

c. **Hearsay** – if the ESI is offered for its substantive truth, is it **hearsay** as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807)
d. **Form of Document/Best Evidence Rule** – is the form of the ESI that is being offered as evidence an **original** or **duplicate** under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008)
e. **Prejudice** – is the probative value of the ESI substantially outweighed by the danger of unfair **prejudice** or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.

III. AUTHENTICATION ISSUES IN GENERAL

a. Authentication is the most significant hurdle for admission of ESI evidence. Emails, texts, social media data, and the like are subject to the same requirements as traditional documents – that is, non-testimonial evidence writings, photographs, and recordings must be authenticated.
b. FRE 901(a) – the authentication process is about proving that the evidence is what it is purported to be
c. FRE 901(b) provides a non-exhaustive list of methods to satisfy this requirement, but most don't apply to ESI. Perhaps this is why ESI "may require greater scrutiny than that required for the authentication of 'hard copy' documents." *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 542-43 (D. Md. 2007)

IV. AUTHENTICATION – CIRCUMSTANTIAL EVIDENCE

a. Circumstantial evidence (FRE 901(b)(4)) – testimony about the distinctive characteristics of a message when considered in conjunction with the surrounding circumstances. A party can authenticate electronically stored information under rule 901(b)(4) with circumstantial evidence that reflects the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence.
b. Emails and text messages have been admitted based on circumstantial evidence. The *Lorraine* court noted that similar uncertainties exist with traditional written documents with signatures that can be forged or distinctive letterhead stationery that can be copied or stolen.
c. A document may be authenticated by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." FRE 901(b)(4).
d. Cases:
    i. *U.S. v. Smith*, 918 F.2d 1501, 1510 (11th Cir. 1990) – ("[t]he government may authenticate a document solely through the use of circumstantial evidence, including the document's own distinctive characteristics and the circumstances surrounding its discovery")
    ii. *U.S. v. Siddiqui*, 235 F.3d 1318, 1322-23(11th Cir. 2000) – emails have been considered properly authenticated when they included the defendant's email address, the reply function automatically included the defendant's email address as sender, the messages contained factual details known to the defendant, and messages included the defendant's nickname and other metadata.
    iii. *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146, 1153-54 (C.D. Cal. 2002) – objections overruled to Internet exhibits printed by a party representative who attached the exhibits to his declaration. The court found

that the dates and web addresses from which the images were printed provided circumstantial indicia of authenticity which, together with the declaration, would support a reasonable juror in the belief that the documents were what plaintiff said they were.

iv. *U.S. v. Safavian*, 435 F.Supp.2d 36 (D.D.C. 2006) – emails were authenticated by distinctive characteristics including email addresses, the defendant's name, and the contents.

V. AUTHENTICATION OF TEXT AND INSTANT MESSAGES BY CIRCUMSTANTIAL EVIDENCE

a. *People v. Pierre*, 41 A.D.3d 289, 838 N.Y.S.2d 546 (1st Dep't 2007) – the court properly received, as an admission, instant message from defendant to victim's cousin; although witness did not save or print the message, it was properly authenticated; defendant's close friend testified to defendant's screen name; cousin testified that she sent instant message to that same screen name, and received reply, content of which made no sense unless it was sent by defendant.

b. *People v. Clevenstine*, 68 A.D.3d 1448, 1450-51, 891 N.Y.S.2d 511 (3d Dep't 2009)

   i. "[A]uthenticity is established by proof that the offered evidence is genuine and that there has been no tampering with it," and "[t]he foundation necessary to establish these elements may differ according to the nature of the evidence sought to be admitted" (*People v. McGee*, 49 N.Y.2d 48, 59 (1979). Here, both victims testified that they had engaged in MySpace instant messaging with defendant about sexual activities; an investigator from the computer crime unit of the State Police related that he had retrieved such conversations from the hard drive of the computer used by the victims; a legal compliance officer for MySpace explained that the messages on the computer had been exchanged by users of account created by defendant and the victims, and defendant's wife recalled the sexually explicit conversations she viewed in defendant's MySpace account while on their computer. Such testimony provided ample authentication for admission of this evidence. *See People v. Lynes*, 49 N.Y.2d 286, 291-293 (1980); *People v. Pierre*, 41 A.D.3d at 291.

c. Other jurisdictions that have directly dealt with the issue of the admissibility of a transcript, or a copy-and-paste document of a text message conversation, have determined that authenticity can be shown through the testimony of a participant to the conversation that the document is a fair and accurate representation of the conversation. *See e.g, United States v. Gagliardi*, 506 F.3d 140 (2d Cir. 2007); *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000) (a participant to the conversation testified that the printout of the electronic communication was an accurate representation of the exchange and had not been altered in any significant manner).

d. *State v. Roseberry*, 197 Ohio App 3d 256 (Ohio Ct. App. 2011) (a handwritten transcript of text messages was properly authenticated through testimony from the recipient of the messages, who was also the creator of the transcript); *Jackson v. State*, 2009 Ark App 466, 320 SW3d 13 (2009) (testimony from a participant to the conversation was sufficient). The testimony of a "witness with knowledge that a matter is what it is claimed to be is sufficient" to satisfy the standard for authentication (*Gagliardi*, 506 F.3d at 151). Here, there was no dispute that the victim, who received these messages on her phone and who compiled them into a single document, had first-hand knowledge of their contents and was an appropriate witness to authenticate the compilation. Moreover, the victim's testimony was corroborated by a detective who had seen the

messages on the victim's phone. *People v. Agudelo*, 96 A.D.3d 611, 947 N.Y.S.2d 96 (1st Dep't 2012).

e. *People v. Givans*, 45 A.D.3d 1460, 845 N.Y.S.2d 665 (4th Dep't 2007) – error to admit cell phone text messages sent to defendant without evidence that he ever retrieved or read it and without authentication of its accuracy or reliability and, further, that it was error to permit jury to access entire contents of the cell phone, including items not admitted into evidence.

VI. AUTHENTICATION BY A PERSON WITH KNOWLEDGE

a. FRE 901(b)(1) allows for authentication through testimony from a witness with knowledge that the matter is what it is claimed to be. Generally, the person who created the evidence can testify to authentication. Alternatively, testimony may be provided by a witness who has personal knowledge of how the social media information is typically generated. Then, the witness must provide "factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of the system or process that does so." *Lorraine*, 241 F.R.D. at 555-56.

b. *Rombom v. Weberman*, 2002 WL 1461890 (S.Ct., Kings Co., 2002, Jones, J.) – emails properly admitted where plaintiff testified that the emails were a compilation of the many he had received as a result of defendant's directions on their websites; that he had received them and printed them out on his office computer; and that they were true and accurate copies of what he had received and printed.

c. *Gagliardi*; 506 F.3d at 151 – chat room logs properly authenticated as having been sent by the defendant through testimony from witnesses who had participated in the online conversations.

VII. AUTHENTICATION BY DISTINCTIVE CHARACTERISTICS

a. A document may be authenticated by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." FRE 901(b)(4); *U.S. v. Smith*, 918 F.2d at 1510 – "the government may authenticate a document solely through the use of circumstantial evidence, including the document's own distinctive characteristics and the circumstances surrounding its discovery")

b. *Griffin v. Maryland*, 19 A.3d 415 (Md. 2011) – in a murder trial, the prosecution's attempt to introduce printouts from a MySpace page to impeach a defense witness was unsuccessful because the witness's picture, date of birth, and location were not sufficiently distinctive to authenticate the printout. The trial court had given "short shrift" to concerns that someone other than the putative author could have accessed the account and failed to acknowledge the possibility that another user could have created the profile at issue.

    i. The *Griffin* court suggested three types of evidence to satisfy the authenticity requirement:

        1. Ask the purported creator if he/she created the profile and added the post in question
        2. A search of the computer of the person who allegedly created the profile, examining the hard drive and internal history to determine if that person originated the profile
        3. Obtain information directly from the social networking website itself to establish the author

ii. *Tienda v. State,* 2010 Tex App Lexis 10031 (2010) – MySpace evidence was admitted. The court noted that (1) the evidence was registered to a person with the defendant's nickname and legal name; (2) the photographs on the profiles were of the defendant; and (3) the profiles referenced the victim's murder and the defendant being arrested. The more particular and individualized the information provided about ESI, the greater the support for a reasonable juror's finding that the person depicted supplied the information.

c. Taken together, *Griffin* and *Tienda* show that if the characteristics of the communication proffered as evidence are genuinely distinctive, courts are likely to allow circumstantial authentication based upon content and context. Conversely, if the characteristics are general, courts may require additional corroborating evidence.

VIII. **AUTHENTICATION OF EMAILS**

a. In general, anyone with **personal knowledge** of an email, including the sender and recipient, can authenticate it.
   i. *U.S. v. Safavian*, 644 F.Supp. 2d 1 (D.D.C. 2009) explains the rationale: "As appellant correctly points out, anybody with the right password can gain access to another's email 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 stationery can be copied or stolen.... 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 is then an adequate foundational showing of their relevance and authenticity."

b. **Email headers** – email headers that include the electronic address of the sender are usually enough to authenticate

c. **Email thread** – if an email was a reply to someone, the digital conversation could serve as the basis of authentication. *Siddiqui*, 235 F.3d 1318.

d. **Comparison** – FRE 901(b)(3) permits authentication by comparison – that is, a court can authenticate an email by comparing it to those previously admitted. The proponent can then ask the court to take judicial notice of the earlier admitted emails.

e. **Discovery production** –
   i. The fact that a party opponent produced emails during discovery can serve as a basis for authentication of the subject emails.
   ii. The production in response to a request for production is inherently an admission of the authenticity of the documents produced. *John Paul Mitchell Systems v. Quality King Distributors, Inc.*, 106 F.Supp.2d 462 (S.D.N.Y. 2000). Therefore, it is good practice to inventory all documents received during discovery, bates-stamp them, and send a confirmatory letter of what was produced (if the other side did not already provide a detailed inventory).

f. **Testimony of sender** – establish (1) that the email address is that of the claimed recipient; (2) the purpose of the communication; (3) if applicable, that the sender received an earlier email and replied to it; (4) that the email was actually sent, and (5) that the recipient acknowledged receipt or took action consistent with an acknowledgment of receipt.

g. **Testimony of recipient** – steps: (1) recipient to acknowledge receipt of email; (2) establish that the sender's email address is that indicated on the face of the email; (3)

compare earlier emails received by the sender; (4) identify logos or other identifying information; (5) establish whether the email was a reply to one sent earlier; (6) establish any conversations with the sender concerning the communication; (7) establish any actions taken by the sender consistent with the communication.

h. **Alteration issues** – the party opposing the admission of an email may claim it was altered or forged. Absent specific evidence showing alteration, however, the court will not exclude an email merely because of the possibility of an alteration. *See, e.g., U.S. v. Safavian*, 644 F.Supp.2d 1 (2009) – "the possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as matter of course; any more than it can be the rationale for excluding paper documents (and copies of those documents)."

i. **Replies** – if a person sends a letter to another person, and after receiving it the recipient replies, the reply letter provides some evidence of authentication of the initial letter. Under this doctrine, as applied to emails, the proponent must show that the author prepared the email, the recipient received it, the recipient replied to it, and the content referred to the first email.

j. **Content** – a proponent of an email may authenticate it by showing that only the purported author was likely to know the information reflected in the message. Examples: the substantive content of the message might be information only known to the purported sender; if the recipient used a reply feature to respond, the new message will include the sender's original message; if the sender sent the message to only one person, its inclusion in the new message indicates that the new message originated with the original recipient.

k. **Action consistent with the message** – after receipt of the email message, the purported recipient takes action consistent with the content of the message – for example, delivery of the merchandise mentioned in the message. Such conduct can provide circumstantial authentication of the source of the message.

IX. AUTHENTICATION OF TEXT AND INSTANT MESSAGES

a. **By testimony of sender.** Steps:
   i. Establish the context of a message – why was sent, its purpose, etc.
   ii. Establish that the number it was sent to was that of the recipient.
   iii. Identify a photograph of the actual text that was sent.
   iv. Describe the process of taking the photograph – who took it, what camera was used, was it an accurate reproduction of the actual text, etc.
   v. Identify and offer transcript of the actual text including how the transcript was made – based on the actual text, reviewed by the sender, verified to be an accurate reflection of the actual text.

b. Establish if there was any responsive text received or any verbal acknowledgment by the recipient in relation to the text sent.

c. **By testimony of recipient.** Steps:
   i. Have the witness acknowledge recognition of the number, digital signature, or name of the person from whom they received a message.
   ii. Establish the basis of the witness's knowledge of the sender's number(e.g., history of text messages with that person)
   iii. The context of the communication (reply to earlier text) or establish the topic that was the subject of the text
   iv. If a photograph was used, establish who took the photo, what camera was used,

whether it was an accurate reproduction of the text

v. Identify and offer transcript of the actual text including how the transcript was made based on the actual text, reviewed by the sender, verified to be an accurate reflection of the actual text.

X. **AUTHENTICATION OF WEBSITES AND SOCIAL MEDIA**

a. Generally: the foundational requirements for authenticating a screenshot from a social media site like Facebook are the same as for a printout from any other website. Essentially, the proponent must offer foundational testimony that the screenshot was actually on the website, it accurately depicts what was on the website, and the content is attributable to the owner. *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534. Some courts require the website owner to provide the necessary foundation to authenticate a page from a website. More liberal courts have held that a printout from a website may be authenticated by a visit to the website. The depiction must accurately reflect the content of the website and the image of the page on the computer and which the screen shot was made. A screen shot from a recognized corporation, such as a bank or credit card company, generally causes less concern that a personal blog posted where a non-owner can more easily manipulate the content. Information from government websites is deemed self-authenticated if the proponent establishes that the information is current and complete.

b. Foundational issues:

   i. Assuming the proponent is not the person whose website posting is at issue, a foundation can be laid by simply having a witness testify that he or she is the person who printed out the posting, he or she recalls the appearance of the printout which was made from the social media site, and that he or she recognized the exhibit as that printout.

   ii. Assuming such a witness is not available, the proponent can have a witness testify that the witness visited the social media site at issue, read the information there that is reflected in the proposed printout exhibit, remembers the contents of the social media site, and can identify the proposed printout exhibit as accurately reflecting the posting that he or she saw

   iii. Totality of the circumstances approach to determine that the social media posting is attributable to a certain person or entity.

   iv. A forensic computer expert testifies that he or she examined the hard drive of the computer used by a particular person and was able to recover the posting from the hard drive of that computer, thereby providing evidence that the exclusive user of that computer was the source of the posting period.

   v. If such a witness is unavailable, other relevant factors include that the printout has adopted the user name shown on the profile page.

   vi. Whether the person has shared his social media password with others.

c. Whether there is a photograph of the person or the profile page identifies a person to whom the proponent wishes to attribute the posting.

d. Whether there is personal information on the profile page such as birthday, unique name, or other pedigree information.

e. Steps: (1) proof that the witness visited the website; (2) when the website was visited; (3) establish that the website was current as opposed to stale sites. For example, postings reflect current information and dates; (4) establish how the site was accessed (i.e., Google search, Internet Explorer, etc.) (5) description of the website access –

identify material on the website including names, addresses, logos, phone numbers, etc.; (6) recognition of the website based on visits; (7) proof that the screen shot was printed from the website and the date and time the screen shot was captured; (8) proof that the screen shot in the printout is the same as what the witness saw on the computer screen; (9) proof that the printout was not altered or modified from the image on the computer.

XI. **MATERIAL AND NECESSARY VS. PRIVACY RIGHTS**

a. *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (S.Ct., Suffolk Co., Spinner, J.) – a plaintiff was required to give the defendant access to her private postings from two social network sites, Facebook and MySpace, that could contradict claims she made in a personal injury action. The defendant was granted access to all social media pages, including all deleted pages and related information as there was indication that the social networking sites contained information inconsistent with her personal injury claims. The information was material and necessary to the defense and/or could lead to admissible evidence. The court found that "Defendant's need for access to the information outweighs any privacy concerns that may be voiced by the Plaintiff."

b. The Court further commented that "when plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of the social networking sites or else they would cease to exist...in this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking."

XII. **SUGGESTED METHODS FOR AUTHENTICATION OF SOCIAL NETWORK PROFILE POSTINGS**

a. Testimony from the purported creator of the social network post
b. Testimony from persons who received the messages
c. Testimony about the contextual clues and distinctive aspects in the messages themselves tending to reveal the identity of the sender
d. Testimony regarding the account holder's exclusive access to the originating computer and social media accounts
e. Expert testimony concerning the results of the search of the account holder's hard drive
f. Testimony directly from the social media site
g. Expert testimony regarding how social media accounts are accessed and what methods are used to prevent unauthorized access

XIII. **JUDICIAL NOTICE OF INFORMATION ON WEBSITES**

a. Example: "The court's computerized records, which were not included in the record but of which we take judicial notice, show that in accordance with the warning in the court's scheduling notice dated November 23, 2004, admittedly received by plaintiff's attorney, the action was dismissed on March 2, 2005 pursuant to 22 NYCRR 202.27 when plaintiff failed to appear for a pre-note of issue conference." *Perez v. New York City Hous. Auth.*, 47 A.D.3d 505, 850 N.Y.S.2d 75 (1st Dep't 2008).

XIV. **AUTHENTICATION OF PHOTOGRAPHS**

a. *People v. Lenihan*, 30 Misc.3d 289, 911 NYS2d 588 (S.Ct, Queens Co., 2010) – defendant precluded from confronting witnesses with printouts of MySpace photos depicting him in gang clothing because of the ability to digitally alter photographs on

the computer. Accordingly, proof that a message or photograph came from a particular account or device without further authenticating evidence is inadequate proof of authorship or depiction.

b. *In re Marriage of Perry*, 2012 IL App (1st Dist) 113054 – the foundation for the admissibility of electronic duplicates of photographs from a website saved on a flash drive could be established under the traditional rules of evidence.

XV. **CLIENT READING SPOUSE'S EMAILS**

a. NYSBA Comm. on Professional Ethics, Op. 945, 11/7/12 – a divorce attorney should not generally reveal to opposing counsel the client's admission that the client has been reading his or her spouse's email messages, unless the lawyer knows that such conduct is criminal or fraudulent. While the lawyer should admonish the client to refrain from this conduct, disclosure should not be made of what the client is doing absent an exception to the general duty to preserve a client's confidential information.

b. New York Rule of Professional Conduct Rule 3.3(b) – a lawyer who represents a client before a tribunal and who knows that a person intends to engage, is engaging, or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

XVI. **ADVICE TO TAKE DOWN A POST**

a. NY County Lawyers' Assn., Ethics Opinion 745 – "an attorney may properly review a client's social media pages and advise the client that certain material is posted on a social media page may be used against the client for impeachment or similar purposes. In advising a client, attorneys should be mindful of their ethical responsibilities under RPC 3.4. That rule provides that a lawyer shall not "(a)(1) suppress any evidence that the lawyer or the client has a legal obligation to produce...[nor] (3) conceal or knowingly fail to disclose that which the lawyer is required by law to reveal...provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, an attorney may offer advice as to what may be kept on "private social media pages, and what may be "taken down" or "removed."

XVII. **COST ALLOCATION – REQUESTER PAYS**

a. *Silverman v. Shaoul,* 30 M.3d 491, 913 N.Y.S.2d 870 (S.Ct., NY Co.; Bransten; J.). Requesting party bears the cost of electronic discovery when the data sought is not "readily available." In this case, the data at issue was neither archived nor deleted but simply stored in a number of places and "interspersed with defendant's various documents for the several business entities." The fact that defendant was required to process the data was not an undue burden, but merely the normal burden of litigation.

b. The Court does not suggest that retrieving archived data is the only circumstance that renders electronic data not "readily available."

c. *Waltzer v. Tradescape & Co., L.L.C.,* 819 N.Y.S.2d 38 (1st Dep't 2006) – the cost of an examination of defendant agents to see if material should not be produced due to privilege or on relevancy grounds should be borne by the producing (not requesting) party.

d. *Lipco Elec. Corp. V. ASG Consulting Corp.,* 4 M.3d 1019(A), 798 N.Y.S.2d 345 (S.Ct., Nassau Co., 2004, Austin, J.) – under the CPLR, the party seeking discovery should incur the costs incurred in the production of discovery material.

e. *Etzion v. Etzion,* 19 M.3d 1102(A), 859 N.Y.S.2d 902 (S.Ct., Nassau Co., 2005, Marber,

J.) – in matrimonial action, plaintiff directed to bear the costs associated with attorney and computer expert time to clone or copy the hard drive of computers of her husband-defendant, as under the CPLR, the party seeking discovery should incur the costs in the production of discovery material.

f. *T.A. Ahern Contractors Corp. v. DASNY*, 24 M.3d 416, 875 NYS2d 862 (S.Ct, NY Co., 2009) – court was not empowered by statute or case law to overturn the well-settled rule in New York that the party seeking discovery bear the cost incurred in this production, and ordered that ESI will not be produced until such time as requesting party agrees to bear the costs associated with its production.

g. Domestic Relations Law §237(d): The term "expenses" as used in subdivisions (a) and (b) of this section shall include, but shall not be limited to, accountant fees, appraisal fees, actuarial fees, investigative fees and other fees and expenses that the court may determine to be necessary to enable a spouse to carry on or defend an action or proceeding under this section.

APPENDIX – SAMPLE Q&A

AUTHENTICATION BY EMAIL THREAD

Q. Would you please identify Defendant's Exhibit D.
A: It is a copy of an email I sent to my employer.
Q: When did you send this email?
A: April 21, 2012.
Q: Under what circumstances did you send this email?
A:. I was replying to an email my employer sent me earlier in the day.
Q: Do you recognize your employer's email address?
A: Yes.
Q: What is his email address?
A: TheBoss@gmail.com.
Q: On the email header does it reflect where this email was sent?
A: Yes.
Q: Where was it sent?
A: TheBoss@gmail.com.

AUTHENTICATION BY TESTIMONY OF EMAIL SENDER

Q: Tell the Court what this document is.
A: It is an email I sent to my friend Bill.
Q: Do you know Bill's email address?
A: Yes.
Q: What is his email address?
A. Bill@gmail.com.
Q: Did you send the email to that address?
A: Yes.
Q: For what purpose did you send the email?
A: I wanted to confirm our dinner plans for that evening.
Q: Did Bill ever acknowledge the email you sent?
A: Yes, he called me an hour after I sent the email to discuss our dinner plans.

AUTHENTICATION BY TESTIMONY OF EMAIL RECIPIENT

Q: Please identify this document.
A: It is an email I received from my attorney.
Q: What is the email address of the sender?
A: GreatLawyer@lawfirm.com.
Q: Do you recognize any identifying marks on the email?
A: Yes, I recognize the logo of the firm where my attorney works and his phone number is on the email.
Q: When did you receive this email?
A: October 5, 2012.
Q: Had you sent your attorney any emails earlier in the day on October 5, 2012?
A: Yes, and this was a reply to an e-mail I sent that morning.
Q: Why did you send your attorney an email in the morning?
A: I was attempting to set up an appointment with him regarding the issue of visitation with my children.

Q: Did you have a conversation with your attorney after you received this email?
A: Yes, I had a phone conversation with him about 10 minutes after I received the email.
Q: What was the topic of the telephone conversation?
A: It concerned the issue of visitation with my children.

AUTHENTICATION BY TESTIMONY OF SENDER OF TEXT MESSAGE
Q: Identify the document.
A: That is a picture of the text message I forwarded to my employer.
Q: What number was the text sent to?
A: 867-5309.
Q: Whose number is that?
A: My employer's number.
Q: When did you send this text?
A: January 10, 2013.
Q: What was the purpose of sending the text to your employer?
A: I wanted to update her on a sale I had just made.
Q: How did you capture the image contained in this exhibit?
A: My brother took a picture of my message on his phone and printed it out for me.
Q: Does that picture accurately reflect how the text looked when you sent it?
A: Yes.

AUTHENTICATION BY TESTIMONY OF RECIPIENT OF TEXT MESSAGE
Q: Would you please identify this document?
A: It is a transcript from a text exchange between me and my wife.
Q: What is a text exchange?
A: It's a series of text messages we sent each other as part of an argument we were having.
Q: When was the exchange?
A: During the evening of April 30.
Q: What was the subject of the conversation?
A: My wife was mad because my girlfriend called her and yelled at her.
Q: Did you ever speak to your wife directly about this matter on that date?
A: Yes, later in the evening I went home and we further argued about this matter.
Q: Tell us how you prepared this transcript.
A: I typed the emails in the order they appeared on my phone.
Q: Is the transcript that's been marked as Defendant's Exhibit F identical to the actual text messages sent on April 30?
A: Yes.
Q: Did you alter or modify in anyway the text messages that appear on the transcript?
A: No.

AUTHENTICATION OF SOCIAL MEDIA PAGE
Q: Are you familiar with the social media website Facebook?
A: Yes.
Q: How are you familiar with it?
A: I have been using it four to five times per week for the last three years.
Q: Generally speaking, what do you do on the website?

A: I keep up with my friends, what they are doing, and special things in their lives.
Q: What is a Facebook friendship?
A: You are permitted to follow certain chosen friends.
Q: How is a Facebook friendship created?
A: You invite someone to be your friend and if the person accepts you become Facebook friends.
A: Was Joan Smith your Facebook friend?
A: Yes.
Q: What is a Facebook wall?
A: This is an area where someone has personal information open only to friends.
Q: How you access someone's Facebook wall?
A: You click their profile.
Q: What type of information is found on Joan Smith's wall?
A: Personal information such as special events, pictures, employment, where she lives, etc.
Q: Have you ever visited Joan Smith's wall?
A: Many times.
Q: Have you done so recently?
A: Yes, I visited it last week.
Q: What did you see on her wall?
A: I saw a picture of her and my husband with their arms around each other at what appeared to be a party, and another picture at the same place where they were kissing.
Q: Did you print a copy of the pictures you saw?
A: Yes.

CM&M CAMPOLO, MIDDLETON & MCCORMICK, LLP

Patrick McCormick heads the firm's Litigation & Appeals practice, which is known for taking on the most difficult cases. He litigates all types of complex commercial and real estate matters and counsels clients on issues including contract disputes, disputes over employment agreements and restrictive and non-compete covenants, corporate and partnership dissolutions, trade secrets, insurance claims, real estate title claims, mortgage foreclosure, and lease disputes. His successes include the representation of a victim of a $70 million fraud in a federal RICO action and of a prominent East End property developer in claims against partners related to ownership and interest in a large-scale development project.

Patrick also handles civil and criminal appeals. Representing clients in both federal and state court, he has argued numerous appeals, including three arguments at the New York State Court of Appeals – the state's highest court. His appellate work includes a successful appeal of a lower court order resulting in an award of legal fees and interest for our client, a major lending institution.

Additionally, Patrick maintains a busy landlord-tenant practice, representing both landlords and tenants in commercial and residential matters. His broad range of services in the landlord-tenant arena includes lease and contract drafting and review, eviction proceedings, rent collection, lease violations, security deposits, habitability issues, and environmental matters. His clients include national commercial shopping centers, retailers, and publicly traded home builders.

Patrick's diverse legal career includes serving four years as an Assistant District Attorney in the Bronx, where he prosecuted felony matters and appeals and conducted preliminary felony and homicide investigations at crime scenes.

Boards, Associations, and Leadership
President, Child Abuse Prevention Services (CAPS)
Board of Directors, Developmental Disabilities Institute (DDI)
Member, Suffolk County Bar Association (SCBA)
Associate Dean and Officer, Suffolk County Bar Association Academy of Law
Co-Chair, Suffolk County Bar Association Appellate Practice Committee
Associate Member, Long Island Builders Institute (LIBI)
Alexander Hamilton Inn of Court
Past Adjunct Professor of Law, Hofstra University, Maurice A. Deane School of Law

Recognitions
2015 - Leadership in Law Award, Long Island Business News
2015 - New York Super Lawyers - Metro Edition
2014 - New York Super Lawyers - Metro Edition
2013 - New York Super Lawyers - Metro Edition
2011 - Who's Who in Commercial Real Estate Law, Long Island Business News

Patrick McCormick, Esq.
Partner

(631) 738-9100
pmccormick@cmmllp.com

EDUCATION
Fordham University, B.A.
St. John's University School of Law, J.D.

ADMISSIONS
New York
United States Court of Appeals, Second Circuit
United States District Court, Southern District of New York
United States District Court, Eastern District of New York
United States Supreme Court

Robert A. Cohen, one of the founding partners of Tabat, Cohen, Blum & Yovino, PC, has practiced matrimonial and family law in Suffolk and Nassau counties for more than 35 years. While his front page New York Law Journal trial decisions and landmark appellate cases reflect his litigation success, Mr. Cohen's focus on the psychology of settlement negotiations also achieves positive results. He was selected to the board of directors of the Suffolk County Matrimonial Bar Association and a member of the prestigious American Inns of the Court. He frequently lectures on custody, equitable distribution and support issues, as well as trial techniques. Mr. Cohen's continuing selection to the Super Lawyers list and achievement of an AV® Preeminent™ Peer Review Rating from Martindale-Hubbell® illustrates the great respect he has earned from his peers and the judiciary.

Honors & Awards:

- Top Lawyer in the NY Metro Area; Super Lawyers (2007- 2015)
- Long Island's Top Rated Lawyer; ALM Legal Leaders (2014- 2016)
- Top Legal Eagle; Long Island Pulse Magazine (2012-2016)
- AV® Preeminent™ Peer Review Rating; Martindale-Hubbell® (2006-2015)
- Rated 10.0 out of 10.0 "Superb"; Avvo (2013-2016)
- Lead Counsel Rated; Thompson Reuters (2014 & 2016)
- Top 10 Attorney Award; The National Academy of Family Law Attorneys (2015)
- Nation's Top 1% Award; National Association of Distinguished Counsel (2015)

Admitted:

- New York, 1980

Education:

- J.D., New York Law School, 1979
- B.A., American University, 1976

Professional Associations:

- Suffolk County Matrimonial Bar Association, Member, Board of Directors
- Suffolk County Bar Association, Member, Matrimonial Committee

We wish to extend a special thank you to Stephen Gassman, Esq. of Gassman Baiamonte Betts, PC for the information he has compiled regarding the admission of electronic evidence.

Hon. James F. Quinn
Suffolk County, County Court
Acting Supreme Court Judge
400 Carleton Avenue
Central Islip, New York 11722
631-853-6162

Elected 2009

Admission to Bar: NYS Appellate Division, Second Dept. - 1984
US District Court, Eastern District of NY - 1984
US District Court, Western District of NY - 2006

Law School: Washburn University (1983 - JD)

Other Education: St. John's University (1978 - BS)

Previous Judgeship: Family Court Judge 2009-2010
Associate Village Justice, Lindenhurst, NY (2006-2008)

Other Professional Experience: Private Practice - Phillips, Weiner & Quinn (1984-2008)
Adjunct Professor - Touro Law School (2010, 2011, 2012, 2013 - Family Law; Advanced Family Law)

Professional and Civic Activities:

Member or Former Member
- Suffolk Academy of Law
- National Council of Juvenile Justice Judges
- Child Abuse & Neglect Institute - 2010
- County Court Judges Association
- NYS Magistrates Association
- NYS Bar Assoc. Mock Trial Tournaments
- New York State Bar Association
- Suffolk County Bar Association
- American Trial Lawyers Association
- Brehon Society
- Board of Directors - Kaitlin Charity Memorial Scholarship
- Board of Directors - Idle Hour Civic Association
- Counsel to Knights of Columbus
- Soccer and Baseball Coach Little League

Published Decisions: Sorrentino v. Sorrentino, NULJ 1/26/12;
Coco v. Coco, 107 A.D.2d 21, 485 N.Y.S.2d 286 (2nd Dept. 1985);
In re Parthe, 230 A.D.2d 850, 646 N.Y.S.2d 825;
Wojnarowski adv. Berlin, 32 A.D.3d 810, 820 N.Y.S.2d 855 (2nd Dept. 2006);
Koehler v. Village of Lindenhurst, 42 A.D.3d 438, 839 N.Y.S.2d 539.

JOHN J. LEO
Supreme Court-County of Suffolk
400 Carleton Avenue, Central Islip, New York 11723
(631) 853-4921

BAR ADMISSIONS

Admitted to practice in New York and before the Supreme Court of the United States, the United States District Court of the Southern, and Eastern Districts.

WORK EXPERIENCE

Justice of the Supreme Court of the State of New York, County of Suffolk
400 Carleton Avenue, Central Islip, N.Y.
January 2013 to the Present

Town Attorney, Town of Huntington,
100 Main Street, Huntington, New York.
January 2002 to December 2012
Chief legal officer for a 200,000 person suburban town with a $180 million dollar budget. Manage and direct a staff of 8 full time attorneys, 8 part time attorneys and an administrative staff of 7 as well supervise various outside counsel. Responsible for employment, contract, personal injury, environmental, transfers of property, licensing, lease, use of public land and property, constitutional, and municipal procedural issues on a regular basis.

Law Offices of John J. Leo, Esq., 191 New York Avenue, Huntington, New York.
March 1992 to 2012.
Areas of concentration: Election Law; labor-management relations in the public and Private sectors; employment litigation Including arbitration, PERB hearings and discrimination matters; civil litigation and general commercial practice.

Manning, Raab, Dealy & Sturm, 440 Park Avenue South, New York, New York. September 1985 to March 1992.
Areas of concentration: labor-management relations including collective bargaining and arbitration, civil litigation, Civil RICO, real estate, trust and estates and general commercial practice. Clients represented include labor unions, a

commercial bank, construction contractors, recycling companies and general commercial enterprises.

Diconza, Larocca & DiCunto, 478 Bayridge Parkway, Brooklyn, New York, September 1983 to September 1985.
General practice including general litigation, real estate and estates.

Lipsig, Sullivan & Liapakis, P.C., 100 Church Street, New York, New York, January 1982 to September 1983

Concentration in commercial and personal injury litigation.

COMMUNITY

St. Hugh's Basketball- Coordinator of and a coach in youth basketball league that has over 1,000 participants. 2001 to 2015

St. Hugh's Soccer-Director of and a coach in youth soccer league that has over 500 participants. 1999 to 2007

Tri-Village Baseball/Softball-Manager of boy's baseball and girls' softball teams as well as coach of the local Williamsport team. 1997 to 2011.

St. Anthony's High School, Huntington, New York, Father's Guild; Chairperson of Father Daughter Dance 2008 to the present

St. Hugh of Lincoln R.C.,
Huntington Station, N.Y.
Trustee 2009 to present.

Suffolk Academy of Law
Director and lecturer
2013 to Present

Suffolk Bar Association
Member

Supreme Court Judges Association
Member

EDUCATION

FORDHAM UNIVERSITY SCHOOL OF LAW, New York, New York, J.D. 1981 Activities: President, Student Body (1980-1981); yearbook and newspaper contributor.

NEW YORK UNIVERSITY GRADUATE SCHOOL OF BUSINESS,
New York, New York M.B.A. 1979
Finance/Accounting

FORDHAM UNIVERSITY, Bronx, New York, B.A. 1976 Economics, cum laude. Activities: Ruby Team (3 years-captain and selector)

References supplied on request.