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

Not Your Mother's Evidence #2: Electronic Evidence

Presenters:

Hon. Mark Cohen
Michael Glass, Esq.
Brian C. Doyle, Esq.
Patrick McCormick, Esq.

Program Coordinators: Cheryl Mintz, Esq., Patrick McCormick, Esq., Hon. John J. Leo

October 20, 2016
SCBA Center - Hauppauge, NY

PATRICK MCCORMICK

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.

Education

Fordham University, B.A.

St. John's University School of Law, J.D.

Admissions

New York

United States District Court, Southern District of New York

United States District Court, Eastern District of New York

United States Court of Appeals, Second District

United States Supreme Court

Boards, Associations and Leadership

Board of Directors, Suffolk County Bar Association

Associate Dean and Officer, Suffolk County Bar Association Academy of Law

President, Child Abuse Prevention Services (CAPS)

Board of Directors, Developmental Disabilities Institute (DDI)

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

Martindale-Hubbell AV Preeminent Rating

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

FARRELLFRITZ P.C.
BECAUSE SUCCESS MATTERS.

Brian C. Doyle

Commercial Litigation

Partner | 631-613-7163 | bdoyle@farrellfritz.com

LOCATION: Water Mill

Brian C. Doyle is a partner concentrating his practice in business, commercial and state court criminal litigation. Mr. Doyle represents large and small businesses, including commercial landlords, in litigated matters throughout Nassau and Suffolk County. Mr. Doyle has also represented individuals in Suffolk County in construction disputes, land use disputes, business and broker disputes, adverse possession claims and justice, district and county court criminal matters.

Prior to joining Farrell Fritz, Mr. Doyle spent four years associated with a law firm in Southampton, New York, where he handled residential and commercial real estate transactions, landlord-tenant litigation, commercial and criminal litigation.

After graduation from law school, Mr. Doyle served as an Assistant District Attorney in the Suffolk County District Attorney's Office, where he received the Outstanding Prosecutor Award while an Assistant in the East End Bureau.

Mr. Doyle earned his Juris Doctor degree from the Wake Forest University School of Law in 2000 and his B.A. in political science from the University of North Carolina at Chapel Hill in 1997. Mr. Doyle is a member of the New York State and Suffolk County Bar Associations and has, for the past several years, chaired the Suffolk Bar Association's East End Committee. Brian is a frequent lecturer to East End real estate brokers on issues related to leasing, commercial litigation and evictions and has lectured the Suffolk County Bar on handling landlord-tenant disputes.

Mr. Doyle is admitted to practice in New York State and in the United States District Court for the Eastern District of New York. He has an AV Preeminent Martindale-Hubbell Peer Review Rating.

Office
Water Mill
50 Station Road Building 1
Water Mill, NY 11976

Practice Areas
Commercial Litigation

Education
University of North Carolina at Chapel Hill
Wake Forest University School of Law

ADMISSIBILITY OF ELECTRONIC EVIDENCE

Presented by Patrick McCormick, Esq.
Chair, Litigation & Appeals Department
Campolo, Middleton & McCormick, LLP

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 cautions:

> 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. **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.

II. **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)

III. **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.

IV. 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.

V. 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.

VI. 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.

VII. 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.

VIII. 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.

IX. THE "I DIDN'T SEND IT" ARGUMENT

a. How do you authenticate an email or text message when the witness/purported author or sender of the message will not back away from the claim that he/she did not author or send the email/text message?
    i. It is possible for someone to remotely send an email or text message from your computer or cell phone. There are apps (i.e., AirDroid) that allow remote access to cell phones and remote access to computers. It is also possible to delete individual text messages from iPhones; there are also apps (i.e. "Fake SMS," "Edit SMS," "reTxt") that allow text messages to be edited and deleted.
    ii. Thus, when the purported author/sender of a text message or email denies actually preparing or sending the message, the authentication process takes a different turn that may require expert analysis of the phone or computer or obtaining records from a service provider to establish whether and when messages were sent.
    iii. Additionally, the purported author/sender of the text message or email should be questioned, ideally during discovery, regarding:
        1. Whether any other person had knowledge of the purported sender's login information (user name and password);
        2. Whether anyone had access to the purported sender's cell phone or computer during the time in question; and
        3. Whether any particular app that allows for remote access to cell phones or editing text messages was downloaded and perhaps subsequently deleted from the cell phone. This may require expert testimony.
    iv. Similarly, a screen shot of a text message or email may not tell the whole story. You must be cognizant of the potential for "spoofing" (the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source). While email spoofing is a tactic usually used in phishing or spam campaigns to induce someone to open an email so that a virus can be transmitted (because people are more likely to open an email when they think it was sent from a legitimate source), the possibility remains that the same tactic can be used to create the appearance, for litigation purposes, that a particular person sent an email when in fact such is not the case.

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 BY TESTIMONY OF "SENDER" OF TEXT MESSAGE WHO DENIES SENDING IT
Q: Do you recognize this text message sent from your account at 8:02 p.m. on October 17, 2012?
A: No.
Q: Is your cell phone number 867-5309?
A: Yes.
Q: Could you please read the phone number that this text message purports to be from?
A: 867-5309. But I didn't send it.

Q: Did you send a message at 8:00 p.m. on that date?
A: Yes.
Q: Did you send a message at 8:08 p.m. on that date?
A: Yes. But not at 8:02.
Q: Does this message at 8:02 p.m. reference a soccer game?
A: Apparently.
Q: Do the messages at 8:00 and 8:08 reference a soccer game?
A: Yes.
Q: At the time this text message was purportedly sent on October 17, 2012, did anyone have access to your phone other than you?
A: No.
Q: Had you ever lost your phone or any phone associated with this number?
A: No.
Q: At the time, did anyone have access to any of your computers or other devices?
A: No.
Q: Was your phone password or access code ever written down anywhere?
A: No.
Q: Did anyone in your office have access to your phone password or access code?
A: No.
Q: At the time, did anyone have the login information for your phone?
A: I don't think so.
Q: Have you ever deleted any apps from your phone?
A: Not that I can recall.
Q: Have you ever changed or modified any text messages that you sent?
A: No.
Q: Have you ever changed or modified any text messages that you received?
A: No.

QUESTIONING OF EXPERT REGARDING WITNESS WHO DENIES SENDING A MESSAGE
Q: Did you examine the cell phone that purportedly received the text message in question?
A: Yes.
Q: Did you find this text message on the phone?
A: No, but that in itself does not mean that the message was not received by the phone.
Q: How is that possible?
A: This is an iPhone, so it's possible to delete entire text message conversations or even individual messages sent during a conversation. That doesn't mean the message was never received.
Q: During your examination of the phone, did you find evidence of any apps that could be used to edit text messages?
A: No such apps were on the phone at the time of my examination, but I did find other evidence.
Q: What other evidence did you find?
A: I reviewed the [purported recipient's] purchase history in the App Store, and on November 20, 2012, an app called Fake SMS was purchased and downloaded.
Q: What does this app do?
A: This app allows you to edit text messages that have already been received.
Q: So what does this finding tell you?
A: It is possible that the "recipient" of this message edited a text message sent by the "sender" to reflect a different date, time, and message than what was actually sent. The recipient could have then deleted the Fake SMS app from the phone.

Q: Did you examine anything else during your investigation?
A: Yes, I examined the recipient's iCloud account.
Q: What were your findings?
A: I was able to retrieve messages that were deleted from the phone but saved in the iCloud account.

QUESTIONING OF EXPERT REGARDING AUTHENTICATION OF EMAIL

Q: Did you examine the email account of the person who allegedly sent the email in question?
A: Yes.
Q: Did you find any evidence of this email in the email account?
A: No.
Q: Did you examine the computer hard drive of the person who allegedly sent the email?
A: Yes, I did.
Q: What did your examination of the hard drive tell you about the activities of that computer on the evening of April 21, 2014?
A: My examination revealed that an account named "Dad" logged in at 7:05 p.m.
Q: How many users had accounts on that computer?
A: Four. There were different logins and passwords for accounts called Dad, Mom, Son, and Daughter.
Q: Did any of the other users log in that evening?
A: Daughter logged in at 10:02 p.m.
Q: What activity was recorded under Dad's account that evening?
A: An email was sent from Dad's email account at 7:08 p.m., at 7:15 p.m., and 7:20 p.m.
Q: What activity was recorded under Daughter's account that evening?
A: There was a visit to Facebook at 10:03 p.m. to 10:10 p.m., then the user logged off.

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
Board of Directors, Suffolk County Bar Association
Associate Dean and Officer, Suffolk County Bar Association Academy of Law
Co-Chair, Suffolk County Bar Association Appellate Practice Committee
President, Child Abuse Prevention Services (CAPS)
Board of Directors, Developmental Disabilities Institute (DDI)
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
Martindale-Hubbell AV Preeminent Rating
Leadership in Law Award, Long Island Business News (2015)
New York Super Lawyers - Metro Edition (2015)
New York Super Lawyers - Metro Edition (2014)
New York Super Lawyers - Metro Edition (2013)
Who's Who in Commercial Real Estate Law, Long Island Business News (2011)

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

Located in both the heart of Long Island and on the East End, Campolo, Middleton & McCormick, LLP is Suffolk County's premier law firm. Over the past generation, our attorneys have played a central role in the most critical legal issues and transactions affecting Long Island. Our commitment to excellence has earned us accolades from the business community, including the prestigious HIA-LI Business Achievement Award and LIBN Corporate Citizenship Award, a spot on the U.S. News & World Report list of Best Law Firms, and the coveted title of Best Law Firm on Long Island.

CM&M

CAMPOLO, MIDDLETON & MCCORMICK, LLP

SUFFOLK COUNTY'S PREMIER LAW FIRM

Corporate | Criminal Defense | Economic Development | Environmental & Land Use | Healthcare
Intellectual Property & Technology | International Regulation, Enforcement & Compliance
Labor & Employment | Liability Insurance & Insurance Coverage
Litigation & Appeals | Mergers & Acquisitions | Municipal Liability | Personal Injury
Real Estate | Retail | Startups | Trusts & Estates, Tax & Elder Law | White Collar Defense & Investigations

4175 Veterans Memorial Highway, Suite 400 | Ronkonkoma, New York 11779
2495 Montauk Highway | Bridgehampton, New York 11932
Phone (631) 738-9100 | Fax (631) 738-0659
www.cmmllp.com

Bethpage BEST OF L.I. 2016

Attorney Advertising

Best Lawyers BEST LAW FIRMS U.S.News 2016

MICHAEL GLASS

Michael Glass has been litigating personal injury and medical malpractice cases for more than 30 years. He has been involved in many cases resulting in million and multimillion-dollar recoveries. Michael graduated magna cum laude from St. John's University (which he attended on a sports scholarship), with a 3,989 average. He therefore attended St. John's University School of Law on a full academic scholarship. Michael graduated from St. John's Law School third in his class. During that time, he served as an editor of the St. John's Law Review, the school's law journal, and received the New York State Trial Lawyers' Louis Harolds Award for Excellence in the field of Tort Law.

Michael has been a partner with RGLZ since 1988, and concentrates in the prosecution of complex personal injury, medical malpractice, and nursing home abuse cases. He regularly lectures to other lawyers on a variety of personal injury topics for the various New York State Bar Associations. He has also published seminary pieces for the New York State Bar Association on several trial-related subjects. He was admitted to the Bar in 1982, and is a member of the Suffolk County Bar Association, the New York State Trial Lawyers Association, the American Association for Justice, and the Nassau/Suffolk Trial Lawyers Association. He and his wife Maureen, also a lawyer, have three children, including RGLZ Associate Attorney Christopher Glass.

SUFFOLK COUNTY BAR ASSOCIATION
ELECTRONIC EVIDENCE SEMINAR

MICHAEL GLASS
RAPPAPORT ,GLASS,
LEVINE & ZULLO, LLP*
1355 Motor Parkway
Islandia, New York 11749
631-293-2300 ext. 112
mglass@rglzlaw.com

ADMISSIBILITY OF SOCIAL MEDIA PAGES- A PRACTICAL APPROACH

I. OVERVIEW

There has been exponential growth in the use of social media sites over the last decade. One study suggested that more than 90% of adults use electronic communication on a daily basis. Social networking sites such as FACEBOOK, LINKED-IN and TWITTER are ubiquitous. FACEBOOK now claims over one billion active users. The sheer number of visits FACEBOOK hosts every day make it exceedingly probable that some of the electronic communications on social networking sites are going to become relevant in the courtroom. Indeed, it is now standard practice for civil and criminal litigators to scour the web, and particularly social media sites, to harvest personal information about parties in the lawsuit. These sites permit the exchange of photographs, messages and profile content, all of which can be fertile ground for cross examination. Surprisingly, there is a dearth of New York State court cases which discuss admissibility standards for social media pages, although many state and federal courts have wrestled with E-evidence admissibility issues.

So, assume you have discovered some very useful information on an adverse party's FACEBOOK page. It may be a message, a post or photographs. If you can get it into evidence, it will materially advance your cause. It is time to consider just how you are going to lay a foolproof foundation for that killer evidence.

The litigator needs to be able to answer three principal questions when considering the admissibility of electronically stored evidence ("ESI") from social media sites:

1. Is the ESI evidence legally **RELEVANT?**

2. Is the ESI evidence **HEARSAY?**

3. By what method am I going to **AUTHENTICATE** the ESI evidence?

The answers to each of these important questions is discussed below.

IS THE SOCIAL MEDIA SITE EVIDENCE LEGALLY RELEVANT?

All evidence must be RELEVANT to be admissible. Evidence is relevant if it tends to prove the existence or non- existence of a material fact in issue in the case. *See Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007); People v. Primo, 96 N.Y.2d 351, 728 N.Y.S.2d 735 (2001). Obviously, this definition is quite broad, but is not without its limitations.

A FACEBOOK page can have vast amounts of information, and some of it may be contradictory to a party's prior testimony or position on trial, but of no legal relevance to the issues in contention. For example, in *People v. Singleton*, 139 A.D.3d 208, 29 N.Y.S.3d 358 (1st Dep't 2016), the criminal convictions of alleged gang members on weapons charges were reversed, in part, because the prosecutor admitted into evidence FACEBOOK posts in which the defendants boasted of firing guns in unrelated incidents and referenced gang affiliations. The prosecutor also introduced photographs showing the defendants holding guns and making gang signs. The Court reversed the convictions, finding the posts were not relevant to the legal issues before the jury and were offered only to demonstrate that defendants had a general propensity to violence.

Similarly, in *People v. Johnson*, 51 Misc. 3d 450, 28 N.Y.S.3d 783 (County Ct Sullivan County 2015), a case involving sexual crimes by a step-father against his minor step-daughter, the Court refused to admit sexually explicit photographs and "likes" of sexually suggestive photographs purportedly from the victim's FACEBOOK account because the posts were not legally relevant to any defense to the charge of Predatory Sexual Assault on a Minor, and were only being used to demonstrate the victim's general sexual proclivity.

Another rule to keep in mind when considering using a social media page to cross-examine a witness is the **collateral evidence rule**. A cross-examiner seeking to impeach a witness is bound by the witness' answer regarding collateral matters and cannot introduce extrinsic evidence (the FACEBOOK page), or call other witnesses, to contradict the witness' testimony on that collateral matter. In *People v. Johnson*, *supra*, the victim-witness took the position that she did not have pornographic material on her FACEBOOK site. The court found that the defendant would not, in any event, be permitted to introduce contrary extrinsic evidence from the victim's FACEBOOK page because impeachment on that ground was collateral to the issues in the case.

Stated simply, digital evidence, like all evidence, must have a tendency to prove or disprove a fact which is of legal consequence to the trial. If it does not, it is irrelevant and it is not going into evidence.

IS THE SOCIAL MEDIA EVIDENCE HEARSAY?

Unless they are photographs or drawings, FACEBOOK pages, TWITTER post and other social media messages are digital, written statements of one kind or another. To be admissible, the proponent of the writings must consider whether the statements are hearsay. If they are, the next inquiry is whether some exception to the hearsay rule saves the evidence.

"**Hearsay** is **defined** in New York and in most jurisdictions, including the federal courts, as an out-of-court statement that is offered to prove the truth of the matter asserted in the statement." *People v. Foster*, 190 Misc.2d 625, 628-629, 740 N.Y.S.2d 567, 569-570 (N.Y. City Crim. Ct. 2002) (citing Martin, Capra and Rossi, New York Evidence Handbook §8.1 [1997]; *People v Nieves,* 67 NY2d 125; Fed Rules of Evid rule 801 [c]). "At the trial level if evidence is **hearsay**, and no exception to the rule is applicable, the evidence must be excluded upon appropriate objection to its admission." *Id.* (citing Prince, Richardson on Evidence § 8-101 [Farrell 11th ed 1995].) Hearsay alarm bells should go off in every case in which the social media evidence is a written statement, especially when the statement was made by a party not involved in the litigation.

Fortunately for the proponents of such evidence, there are more than a few potentially relevant exceptions to the hearsay rule. The most likely exceptions the litigator should consider are:

1. The post or message is a **party admission**. Remember, this hearsay exception requires that the statement be a statement made by a party to the litigation adverse to his/her position on trial. *See, e.g., Murray v. Donlan*, 77 A.D.2d 337, 433 N.Y.S.2d 184 (2d Dep't 1980).

2. The post or message is **not being offered for the truth of its contents**, but to establish notice, motive, or the declarant's state of mind. *See Hopkins v. Amtrak*, 2016 U.S. Dist. LEXIS 57236 (EDNY 2016) (text messages were not hearsay because they were offered to prove state of mind of declarant); *Rombom v. Weberman*, 2002 N.Y. Misc. LEXIS 769, 2002 NY Slip Op 50245(U) (N.Y. Sup. Ct. June 13, 2002) *aff'd.* 309 A.D.2d 844 (2d Dep't 2004) (e-mails were not hearsay because plaintiff introduced the e-mails to establish their effect upon plaintiff, as opposed to the truth of their content).

3. **The post or message reflects an excited utterance or a present sense impression**. Social media messages posted or tweeted contemporaneous with an unfolding event are not at all uncommon. "' **Excited utterances'** are the product of the declarant's exposure to a startling or upsetting event that is sufficiently powerful to render the observer's normal reflective processes inoperative. '**Present sense impression**' declarations, in contrast, are descriptions of events made by a person who is perceiving the event as it is unfolding. They are deemed reliable not because of the declarant's excited mental state, but rather because the contemporaneity of the communication minimizes the opportunity for calculated misstatement as well as the risk of inaccuracy from faulty memory. In our State, we have added a requirement of corroboration to bolster these assurances of reliability. Thus, while the key components of 'excited utterances' are their spontaneity and the declarant's excited mental state, the key components of 'present sense impressions' are contemporaneity and corroboration." *People v. Vasquez*, 88 N.Y.2d 561, 574-575, 647 N.Y.S.2d 697, 703 (1996) (citations omitted).

4. The post or message qualifies as a **business record** made and kept in the regular course of business. See CPLR 4518. "To constitute a business record exception to the hearsay rule, the proponent of the record must first demonstrate that it was within the scope of the entrant's business duty to record the act, transaction or occurrence sought to be admitted. But this satisfies only half the test. In addition, each participant in the chain producing the record, from the initial declarant to the final entrant, must be acting within the course of regular business conduct or the declaration must meet the test of some other hearsay exception *(Johnson v. Lutz*, 253 N.Y. 124, 128; *Toll v. State of New York*, 32 A.D.2d 47, 50). Thus, not only must the entrant be under a business duty to record the event, but the informant must be under a contemporaneous business duty to report the occurrence to the entrant as well (Richardson, Evidence [10th ed -- Prince], § 299)." *Murray v. Donlan*, 77 A.D.2d 337, 345-346, 433 N.Y.S.2d 184, 189 (2d Dep't 1980).

5. The post or message constitutes a **dying declaration** (the last text message from a victim in extremis before crossing the digital divide). See generally 3-155 Bender's New York Evidence § 155.06 (2015).

6. The "statement" in question was not generated by a human, but by a computer. **Computer generated statements** are not hearsay because they do not emanate from a human, but rather from a computer process. For example, FACEBOOK, through its software processes, automatically generates certain information with each message, like the date and time the message was sent. The date and time information is not hearsay because it was not generated by a human. *See People v. Johnson*, 51 Misc.3d 450, 28 N.Y.S.3d 783 (County Ct Sullivan County 2015); *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).

HOW CAN I AUTHENTICATE THE ELECTRONIC EVIDENCE?

If the evidence is relevant and not precluded by the hearsay rule, the next hurdle is authentication. Authentication is perhaps the most important and problematic step in admitting social media posts, profiles or ESI messaging into evidence. Authentication simply means that the party offering the evidence can prove the item is what it purports to be.[1] That can sometimes be easier said than done in the context of social networking pages.

A FACEBOOK page can be faked of "spoofed." It does not take much computer savvy to set up a phony FACEBOOK page. The user obtains a free email address from YAHOO or HOTMAIL or similar sites. No verification of identity is required. The user then proceeds to FACEBOOK and creates a new account using the free e mail address as the contact e mail for verification. The user can then create a FACEBOOK page in any name desired and post photos and send messages as that alternate person. If the user is enterprising enough, he can use the same method to create "friends" and manufacture a social circle which "sends" messages to each other. Unauthorized users can also gain access to a FACEBOOK account if they know the user's password, or if they access the users device when the individual has remained logged in the account. Thus, establishing the true origin of a FACEBOOK or other social media post or profile can be challenging, a fact recognized in the case law. *See, e.g., Sublet v. State*, 113 A.3d 695 (Md. 2015).

Also, as a practical matter, the proponent of the evidence is not offering the actual FACEBOOK page into evidence, since the page is actually a digital representation on a computer screen. The proponent usually offers a print-out or screen shot of the page. The authenticity of the screen shot or printout must also be addressed.

There are a number of ways of meeting the authentication requirement. Some are easy. Others are complex, expensive or impractical in the context of most civil cases where litigants don't have the same subpoena power as law enforcement agencies. Note, however, that the proponent of the evidence does not have to rule out all possible inconsistencies. The

---

[1] The New York Court of Appeals described the authentication burden of documentary evidence in these terms: "In determining whether a proper foundation has been laid for the introduction of real evidence, the accuracy of the object itself is the focus of inquiry, which must be demonstrated by clear and convincing evidence (*see United States v. Fuentes*, 563 F2d 527, 532, cert den *sub nom. Sansone v. United States*, 434 U.S. 959). Accuracy or authenticity is established by proof that the offered evidence is genuine and that there has been no tampering with it (cf. *People v. Julian*, 41 N.Y.2d 340, 342-343). The foundation necessary to establish these elements may differ according to the nature of the evidence sought to be admitted...mere identification by one familiar with the object, however, will be sufficient "when the object possesses unique characteristics or markings" and any material alteration would be readily apparent *(Id.*; *see People v Flanigan*, 174 N.Y. 356)." *People v. McGee*, 49 N.Y.2d 48, 59-60, 424 N.Y.S.2d 157, 163 (N.Y. 1979).

authentication evidence need only be enough to support a reasonable likelihood that the matter is what the proponent claims it to be. *See People v. Moye*, 2016 N.Y. Misc. Lexis 1553 (Sup. Ct. Queens County 2016).

A social media page can be authenticated by:

- testimony from the **author** of the page;
- testimony from **a third party**, if other corroborating proof is available;
- testimony from a **forensic computer expert** who has examined the party's computer or been given access to the site, or
- testimony from by a **business records custodian** of the social media company which hosts the site.

These authentication possibilities are described in more detail below:

1. **AUTHENTICATION BY AUTHOR**: A social media post, message, or profile page can always be authenticated by the author of the page, who can testify that he or she authored the material and that the copy or screen shot produced in court is a fair and accurate copy of what appears in the social media page on the computer. *See Sublet v. State*, 113 A.3d 695 (Md. 2015) (authentication of social networking evidence can be established by asking the purported creator if he created the profile and if he added the post in question).

   If the ESI is a photograph, the person who took the photograph, or indeed any knowledgeable witness, can testify that the photograph is a fair and accurate representation of what it purports to depict. *See Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 561 (D. Md. 2009) ("Photographs have been authenticated for decades ... by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately represents the scene."); *Burchette v. Abercrombie & Fitch Stores, Inc.*, 2010 U.S. Dist. LEXIS 47043, *26, 2010 WL 1948322 (S.D.N.Y. 2010) (Facebook photos can be authenticated by a witness familiar with what is depicted in the photo);

2. **AUTHENTICATION BY THIRD PARTY**: A social media post or message can also be authenticated by appropriate testimony from a third party; that is, one who did not author the material. *People v. Moye*, 2016 N.Y. Misc. Lexis 1553 (Sup. Ct. Queens Cty 2016) (Facebook messages can be authenticated by different types of circumstantial evidence and the author of the message is not the only qualified witness to testify about the account). There are two categories of third party witnesses who can authenticate the social media page:

   A. **NONEXPERT**: A third person who has access to the social media site or the computer of the party who made the post can authenticate the post or message by establishing:

      i. The witness accessed the owner's FACEBOOK or social media page by typing in the URL, (the web address),
      ii. The witness thereupon observed the website;
      iii. The proffered printed copy of the website page is a fair and accurate rendition of that web page, message, etc. AND

iv. There exists other evidence from that witness or otherwise authenticating the proffered evidence as originating with the site owner.

Evidence tending to corroborate ownership of the site will be different in every case, but may include one or more of the following indicia:

a. A showing of the distinctive nature or features of the site as it correlates with unique information known about the author (ex.- a special nickname, a corporate logo, a catchphrase unique to the author). FRE 901(b)(4); *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000);

b. A showing that the offered message is consistent with other messages made by the author as part of an ongoing sequence of messages and replies, like an e mail thread (otherwise known as the reply letter doctrine). *See United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000); *Sublet v. State*, 113 A.D. 695 (Md. 2015);

c. A showing that the author had made similar statements or posts through other forms of communication (like other social networking sites, or in telephone calls or in face to face conversations) during the relevant time period. *See United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000); *United States v. Safavian*, 644 F. Supp, 2d 1 (D.Dist. Ct 2006);

d. A showing that that the site includes information that only the owner of the site could know. *See Smith v. Charles*, 37 Misc.3d 1229(A) (Sup. Ct. Kings Co. 2012);

e. A showing that that the authenticating witness frequently communicated with the site owner through that same URL address and received messages in return. *See People v. Pierre*, 41 A.D.3d 289, 838 N.Y.S.2d 546 (1st Dep't 2007); and

f. any other available circumstantial evidence which distinctively links the claimed owner to the site.

For example, in *United States v. Encarnacion-Lafontaine*, 639 Fed. Appx. 710 (2d Cir. N.Y. 2016), threatening Facebook messages were properly authenticated by showing that the defendant controlled the Facebook accounts, the messages were all sent from IP addresses connected to computers near defendant's apartment, the pattern of access suggested that all the messaging was controlled by the same person, the same accounts were also used to send messages to other acquaintances of defendant, the defendant had the motive to make the threats and only a limited number of people had access to the information in the messages.

Similarly, in *People v. Pierre*, 41 A.D.3d 289, 838 N.Y.S.2d 546 (1st Dep't 2007), instant messages were authenticated without the internet service provider testifying and without the author of the messages testifying. The foundation for the evidence was laid by the testimony of a close friend of the deceased author who identified the victim's screen name and a cousin of the deceased author who testified that he had sent instant messages to the same screen name and received a reply. Also, the court felt that there was no one who, in the circumstances, had a motive to send fake messages.

B. **FORENSIC COMPUTER EXPERT**: A technical expert who has deconstructed the party's computer or website can authenticate the ESI. In the context of criminal cases, law enforcement agencies often seize computers and cell phones from the defendant or other relevant parties. Forensic computer experts then use highly specialized forensic software and investigative methods to find specific electronic data, including Internet use history, word processing documents, images and social media files. These experts can verify that the message, profile or photograph emanated from the device in question and can authenticate the evidence by connecting the ESI to keystrokes made from that same computer or device. *See Sublet v. State*, 113 A.3d 695 (Md. 2015) (authentication of social networking evidence can be established by searching the computer of the person who allegedly created the profile and examining the computer's internet history and hard drive). In civil litigation, however, litigants rarely have unfettered access to the opposite party's computer, and even in the rare case when they do, the cost of a forensic analysis can be prohibitive.[2]

3. **AUTHENTICATION BY A CUSTODIAN EMPLOYEE FROM THE SOCIAL MEDIA PROVIDER**: As with any documentary evidence which would otherwise be admissible as a business record, the testimony of the corporate custodian of records of the social media company can authenticate the ESI. Ideally, the FACEBOOK, TWITTER, or GOOGLE employee would establish the page's provenance as emanating from the owner's device and testify that the owner's data is maintained by the social media provider in the regular course of its business, that it was the regular course of business to hold such data, and that the record was created at or around the relevant time. *See People v Hughes*, 114 A.D.3d 1021, 1023, 981 N.Y.S.2d 158, 161-162, (3d Dep't 2014) ("the People produced testimony from a Verizon employee confirming that text messages had been sent between certain phone numbers, the victim identified the phone numbers as belonging to her and defendant, and she identified the photographs as depicting text messages she received from him. Defendant's testimony that someone else could have sent the messages from his phone presented a factual issue for the jury, and we discern no basis for setting the jury's determination aside"); *Sublet v. State*, 113 A.3d 695 (Md. 2015) (authentication of social networking evidence can be established by obtaining authentication information directly from the social networking website which would link together the profile and the entry to the person who had created it).

SELF-AUTHENTICATING: Indeed, the FACEBOOK, MY SPACE or social media site page may self-authenticate. Both New York State and Federal practice rules include provisions for self-authenticating business records using appropriate certifications. *See* FRE 803(6), 902; CPLR 3122-a; CPLR 4518.

If certifications can be secured from the social media company, the certifications should establish that the proffered evidence was maintained as a business record in the course of regularly conducted business activities. The certification should also verify that the social media site company maintains the proffered page information when (or soon

---

[2] For a technical perspective from a forensic computer expert on authenticating a FACEBOOK page with forensic expert assistance, *see* *http://www.ncids.com/forensic/digital/Daniel_Getting_Facebook_into_Evidence.pdf*

after) their users post the information through use of the site's servers. *See United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014) (ESI records were admitted because they were self-authenticated as certified business records under FRE 902(11)). Even if the records certification is deemed sufficient, the proponent of the evidence must still adduce other sufficient evidence to connect the website pages to the purported author of the posts. *See United States v. Hassan*, *supra.*

Law enforcement agencies, using their broad subpoena powers, can compel the appearance of witnesses from social media networking companies, and require the companies to produce the content of web pages . In civil litigation, however, it may not be so easy to obtain testimony from the service provider records custodian or even an appropriate certification, because disclosure of web site information by service providers is federally prohibited in many cases.

c. **FEDERAL STORED COMMUNICATIONS ACT** The Federal Stored Communications Act, 18 U.S.C. Sec. 2701, et seq., governs the circumstances under which electronic data service providers may disclose a customer's substantive electronic data, meaning the written and photographic content of customer's web pages. The law broadly prohibits an "electronic communication company" (like FACEBOOK, LINKED IN, etc) or "remote computing services" (like Google, Yahoo, etc.) from divulging the contents of most private communications maintained by, or carried by, the service provider. (18 U.S.C. 2702(a)). Two of the most important exceptions to the non-disclosure rule are disclosure (1) in compliance with appropriate subpoenas from criminal or administrative agencies (with certain qualifications); and (2) made with the consent of a party to the communication, or in some cases, the subscriber. See 18 U.S.C. 2702(b)(2), (b)(3); *Crispin v. Christian Audigier*, Inc., 717 F. Supp.2d 965 (Dist Ct. C.D. Cal. 2010).

So, if you are not the government, don't prepare your civil subpoena for social media content yet. There is no exception in the act permitting the service providers to disclose the website information simply because the disclosure is sought by a civil subpoena. See, e.g., *In re Subpoena Duces Tecum to AOL, Inc.*, 550 F.Supp.2d 606, 611 (AOL may not divulge the contents of electronic communications to State Farm because the statute contains no exception for civil subpoenas); *Viacom International v. YouTube, Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding that the statute prohibits the disclosure of ESI information pursuant to a civil subpoena). FACEBOOK specifically states on its website that it will not comply with civil subpoenas because of the prohibitions in the Stored Communications Act.
See https://www.facebook.com/help/473784375984502. ("Federal law does not allow private parties to obtain account contents (ex: messages, Timeline posts, photos) using subpoenas. *See* the Stored Communications Act, 18 U.S.C. §2701 et seq.")

What is the civil litigant to do? If you have the predicate, in discovery, move to require the adversary to provide an authorization to view his or her web content. That is, compel consent. Otherwise, consider whether you have the "lawful consent of the originator or an addressee or intended recipient of such communication, or a subscriber, in the case of a remote computing service." (18 U.S.C. 2703(b)(3)). More likely than not, if you are not law enforcement, without

an appropriate consent, the social media company will not comply with your subpoena.

Many of the service providers have published their rules of engagement when it comes to disclosure and complying with subpoenas served on them. Google, for example, takes the seemingly unsupportable position that it will only accept subpoenas issued out of Santa Clara, California, Superior Court (home of Silicon Valley). FACEBOOK takes the position that the Stored Communications Act does not allow private parties to obtain content directly from FACEBOOK.

See, for example:

Facebook

- Facebook's subpoena/law enforcement page
  - https://www.facebook.com/help/133221086752707?helpref=search

Instagram

- Instagram's subpoena/law enforcement page
  - https://help.instagram.com/494561080557017/8

Google/YouTube

- Google's subpoena/law enforcement page
  - https://www.google.com/transparencyreport/userdatarequests/legalprocess

For more information in this area, see the ABA Publication, "Social Media Evidence-How to Find it and How to Use It.[3]

---

[3] **FOR FURTHER CONSIDERATION:** In any event, in the last several years, methods and manners of authenticating social networking pages have proliferated. See, e.g., 39 *See, e.g., United States v. Brinson*, 772 F.3d 1314 (10th Cir. 2014) (authentication of Facebook messages); *United States v. Vayner*, 769 F.3d 125 (2d Cir. 2014) (authentication of posts on VK.com, a Russian equivalent of Facebook); *United States v. Hassan*, 742 F.3d 104 (4th Cir.), *cert. denied sub nom. Sherifi v. United States*, 134 S. Ct. 2737, 189 L. Ed. 2d 774 (2014), *and cert. denied*, 135 S. Ct. 157, 190 L. Ed. 2d 115 (2014), *and cert. denied sub nom. Yaghi v. United States*, 35 S. Ct. 192,190 L. Ed. 2d 115 (2014) (authentication of Facebook post); *United States v. Adams*, 722 F.3d 788, 821 (6th Cir. 2013) (authentication of MySpace message); *United States v. Lebowitz*, 676 F.3d 1000 (11th Cir. 2012) (authentication of MySpace messages); *Juror No. One v. Superior Court*, 142 Cal. Rptr. 3d 151 (Cal. Ct. App. 2012) (authentication of Facebook post); *Connecticut v. Eleck*, 23 A.3d 818 (Conn. App. Ct. 2011) (authentication of Facebook messages), *aff'd on other grounds*, 100 A.3d 817 (Conn. 2014); *Parker v. State*, 85 A.3d 682 (Del. 2014) (authentication of Facebook posts); *Moore v. State*, 763 S.E.2d 670 (Ga. 2014) (authentication of Facebook posts); *Stapp v. Jansen*, 988 N.E.2d 234 (Ill. App. 2013) (authentication of MySpace and Facebook messages); *State v. Raskie*, 269 P.3d 1268 (Kan. 2012) (authentication of MySpace messages); *Commonwealth v.Foster F.*, 20 N.E.3d 967 (Mass. App. Ct. 2014) (authentication of Facebook messages); *Smith v. State*, 136 So. 3d 424 (Miss. 2014) (authentication of Facebook messages); *State v. Snow*, 437 S.W.3d 396 (Mo. Ct. App. 2014) (authentication of MySpace message); *State v. Paster*, 15 N.E.3d 1252 (Ohio Ct. App. 2014) (authentication of Facebook posts); *State v. Nance*, 393 S.W.3d 212 (Tenn. Crim. App. 2012) (authentication of MySpace posts); *Campbell v. State*, 382 S.W.3d 545 (Tex. App. 2012) (authentication of Facebook messages); *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012) (authentication of MySpace profile); *State v. Lawrence*, 80 A.3d 58 (Vt. 2013) (authentication of MySpace profile).

PRACTICAL APPLICATION-ATTORNEY CHECKLISTS FOR ADMITTING SOCIAL MEDIA EVIDENCE/EMAILS INTO EVIDENCE

1. **SOCIAL NETWORKING SITE PHOTOGRAPHS**

- Ask the court if you can mark the screen shot or print out for identification. (The Court is likely to ask you to show opposing counsel what you have marked at this point/Do not let the jury see the document until it is in evidence).
- Ask that exhibit be shown to witness
- Ask the witness to identify the document as a photograph.
- If the witness downloaded the photograph, ask how the witness obtained the photograph

  Witness Went to URL Address;
  Observed it to be the party's website;
  Printed out the photograph or took a screen shot of same;
  Is the copy of the photograph/screenshot a fair and accurate depiction of what the witness observed on the computer screen on the social media site.

- Ask the witness if the photograph is a fair and accurate depiction of (whatever it is supposed to depict), connecting the photograph to the owner of the website

OFFER THE PHOTOGRAPH INTO EVIDENCE:
Your honor, I offer this photograph into evidence.
Once the photograph is marked "in evidence," it can be published to the jury.
"Your Honor, may we show the photograph to the jury?"

2. **USING WEB SITE POSTS OR EMAIL MESSAGES OF YOUR CLIENT ON YOUR OWN CLIENT'S WEB PAGE**

- Do you have a Facebook page?
- Is it currently active?
- Who has access to this page?
- Does anyone have authorization to update or edit this page other than you?
- How is the page protected?
- (Hand copy of social media page to witness) do you recognize what I just handed you?
- What is it?
- Does it appear to be a fair and accurate representation of your page?
- Does it appear to be altered in any manner?
- ****Your Honor at this time I would like to enter _____ into evidence as Exhibit__.[4]**

---

[4] See, Introducing Facebook posts and Text Messages, Kortney D. Simmons, https://www.tals.org/files/2013%20EJU%20INTRODUCING%20FACEBOOK%20POSTS%20AND%20TEXT%20MESSAGES_0.pdf

3. USING WEB SITE POSTS OR EMAIL MESSAGES BY CROSS EXAMINING THE AUTHOR OF THE MESSAGES

CASE EXAMPLE:
Embry v. State

In *Embry v. State*, 923 N.E.2d 1 (Ind. App. 3/8/10), the defendant was convicted of felony domestic battery by beating his ex-wife and the Court affirmed the conviction. The defense in an effort to establish self-defense cross-examined the ex-wife about statements she had posted on MySpace about the defendant prior to the alleged battery:

BY [DEFENSE]: ... Prior to Au-April 22nd, 2008 had you ever expressed or communicated in any way that you wanted your ex to die a slow painful death?

A I believe you're referring to my "My Space"...
Q I'm not-I-no, I'm not referring to anything. I'm just asking you a simple question: if you'd ever expressed or communicated in any way that you wanted your ex-husband, Mr. Embry, to die a slow painful death?
A I see it right there on your desk.
Q Okay.
A It's my "My Space" blog.
Q Okay, did you say it?
A I typed it.
Q Okay. But the answer is, did you say it? I mean is that your communication.
A I typed it.
Q Okay. And did you ever express um, or communicate in any way that you wanted to be present and dance the cha-cha around his slow painful death?
A It's all there in the blog.
Q Okay. The answer's a simple yes or no. You said it; you've communicated it some way, did you?
A If you want to put that blog there, I...
Q I'm just asking you a simple question.

BY COURT: Ma'am, will ya just answer the question yes or no?

A Yes, I did.
Q Did you ever refer to Mr. Embry or communicate in any way that he was a worthless bag of monkey shit?
A Yes.
Q Did you ever refer to him as dog piss?
A Yes.
Q Did you ever refer to him as a worm puke stale crusty moldy inhuman horrible human oxygen sucking moron?
A Yes.
Q Did you ever communicate the desire, that because he's older and more stupid than you, he will die way before you do?

A I believe I said please assure me that it was possible that he would pass before me."

4. ADMITTING WEB SITE OR E MAIL MESSAGES USING TESTIMONY FROM THIRD PARTY LAY WITNESS(ES)

A. Ask the Court if you can mark the web page/email for identification.
(The Court is likely to ask you to show opposing counsel what you have marked at this point).
Ask that exhibit be shown to witness.
Ask the witness to identify what the exhibit is.
(a copy of the web page/email of …)
At this stage it is not proper for the witness to testify to the contents of the document, as it is not yet in evidence.

B. Establish how the exhibit is **RELEVANT**
Ask the witness to tell the Court and jury what is the general subject matter of the web page/e mail exhibit, **without divulging its specific contents.**
(e.g. -- it lists the sporting activities of the injured plaintiff; it is my bank statement; it concerns the … (transaction which is the subject matter of the lawsuit))

C. Establish the **AUTHENTICITY** of the Exhibit (Web page/e mail).
This process involves authenticating the exhibit, which is a copy from a computer screen, and next demonstrating that the exhibit is, with reasonable probability, from the owner's website and is not a fake.
If the witness downloaded the page or took the screen shot, establish the following:

The witness went to a computer and entered the URL address associated with the website;
The witness reviewed the contents of the website;
The witness confirms that the offered printout or screenshot accurately reflects the website or email content that the witness has reviewed.

If the authenticating witness is a friend or someone who knows the owner of the page, and the witness did not herself download the page, you can try the following:

Are you familiar with the defendant/plaintiff?
How do you know them?
Are you friends with them on any social media websites?
Are you familiar with his or her FACEBOOK page?
Is it currently active?
Would you recognize his/her profile page if it were presented to you today in Court?
Mark page for identification/Hand page to the witness.
Do you recognize what I just handed to you?
What is it?
Does it appear to be a fair and accurate representation of _____'s FACEBOOK page?
Does it appeared to be altered in any manner?

Your Honor, I move to admit this exhibit into evidence.[5]

If there is an objection on authenticity grounds, you can further connect the owner of the website to the exhibit using as many of the below identifiers as possible:

URL is known to the witness as the owner's URL;
The witness previously communicated with the owner using the same URL;
The witness accessed the site using the owner's password;
The exhibit includes the owners screen name/real name;
The exhibit includes owner's corporate logo;
The exhibit includes owner's nickname, catchphrase or other identifier;
The exhibit's contents include information known only to owner or to a few people;
The exhibit is part of, and consistent with, a continuing e mail thread of messages and replies;
The owner of the site made similar or consistent statements in other electronic media, by telephone or in personal conversations;
Other witnesses send and/or received messages from the same URL as messages from the owner;
There is no known reason to suspect the site is a phony social media page or a "spoofed" page or email.

Remember that authenticity can be established in any way that shows the web site or e-mail is genuinely from the owner, and is not a phony or fake. Provide as much confirmatory information as possible.

5. **FOUNDATION USING THE BUSINESS RECORDS EXCEPTION TO THE HEARSAY RULE:**

Are you familiar with Exhibit A for identification?
Can you identify this document?
Was this document prepared in the regular course of the business of your company?
How is this data maintained after it is created/downloaded/received?
Is it the regular course of your business to maintain this data?
How was this document retrieved to create Exhibit A?
Witness should explain how the contents of the exhibit are connected to the website's owner.
Does this exhibit accurately reflect what you retrieved from that webpage?

CONCLUSION

The proponent of social media evidence must consider the obstacles to admission well before trial and plan accordingly. The lawyer must overcome relevancy, hearsay and

---

[5] (See, Introducing Facebook posts and Text Messages, Kortney D. Simmons, https://www.tals.org/files/2013%20EJU%20INTRODUCING%20FACEBOOK%20POSTS%20AND%20TEXT%20MESSAGES_0.pdf

authentication objections. As a practical matter, in most civil cases, the litigant will authenticate social media pages through the testimony of the author of the page, or with a third party familiar with the page, supplemented by corroborating proof of page ownership.

E-evidence can have a substantial impact at trial. Careful planning before trial is the key to its admissibility.

Michael Glass*
Rappaport, Glass, Levine & Zullo
1355 Motor Parkway
Islandia, New York 11749
631 293 2300
Mglass@rglzlaw.com

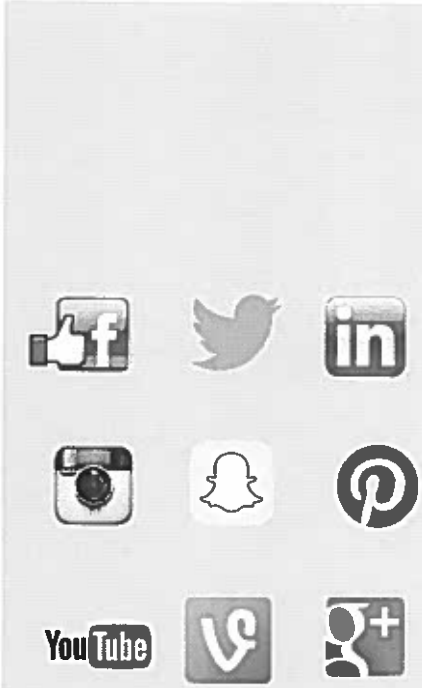
The assistance of Christopher Glass, Esq. in the preparation of this article is greatly appreciated.

Admitting Social Media Evidence

Michael Glass, Esq.

Rappaport, Glass, Levine & Zullo, LLP.

October 20, 2016



Admissibility Issues

- Is the ESI evidence legally relevant?
- Is the ESI evidence hearsay?
- How can I authenticate the ESI exhibit?

People v. Singleton

People v. Johnson

Relevance

Impeachment on a Collateral Matter:

Rule: The collateral evidence rule bars the contradiction of a witness's answers concerning collateral matters by the introduction of extrinsic evidence (eg.-Facebook page) for the sole purpose of impeaching credibility

Hearsay

Hearsay

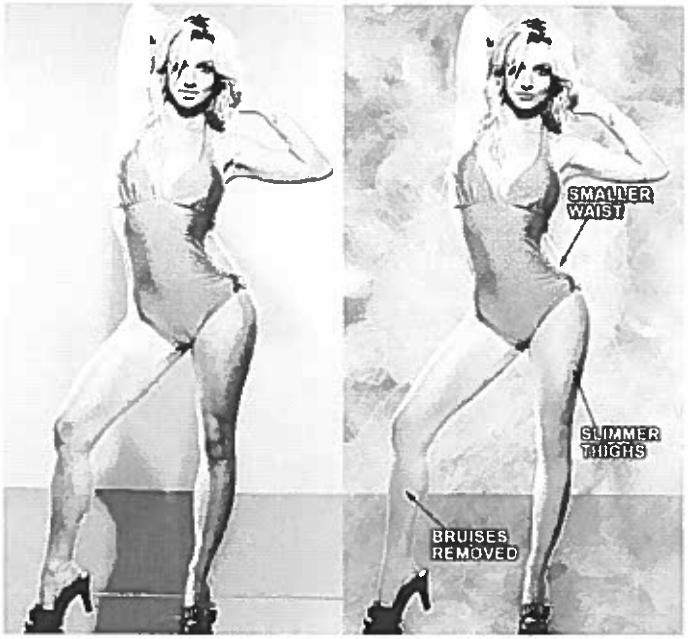
- A statement made out of court that is offered in court to prove the truth of the matter asserted.

Hearsay Exceptions

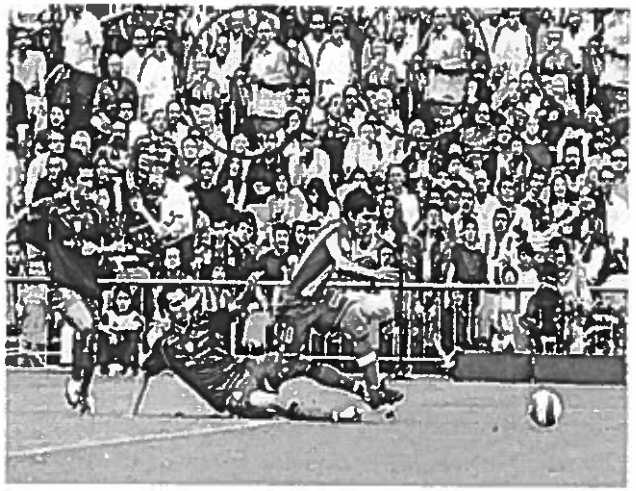
- Party admissions
- Excited utterance / present sense impression
- Business record
- Dying declaration
- Computer generated statements
- Others

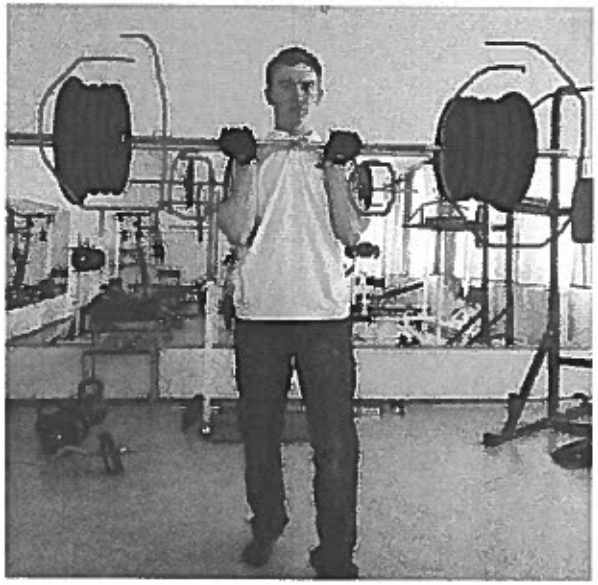
The Authentication Hurdle

Authentication of Photographs



The Power of Editing





Authenticating Photographs from Social Media Sites

Authentication of Electronic Text by Third Party witnesses

Witness **must** confirm the exhibit is a fair **and** accurate copy of the web page.

Other evidence must additionally connect the page as originating with site owner.

Corroborating Evidence (examples)

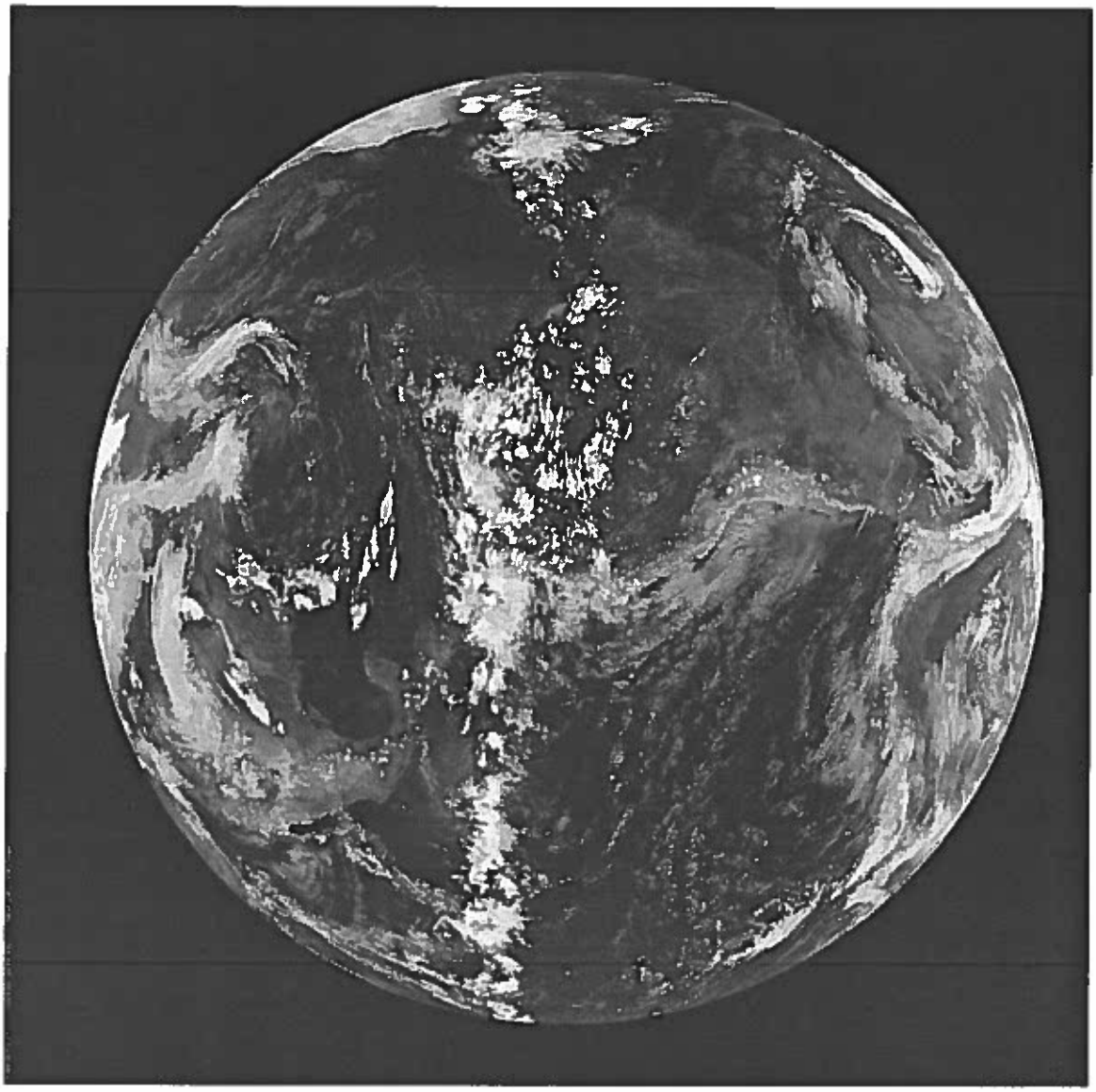
- Distinctive Features of The Message (logos, etc.).
- Part on an ongoing E-Mail thread.
- A showing that author has made similar statements in the past.
- Information in the post only site owner could know.
- Evidence that the authenticating witness had communicated to site owner through that URL address in past.

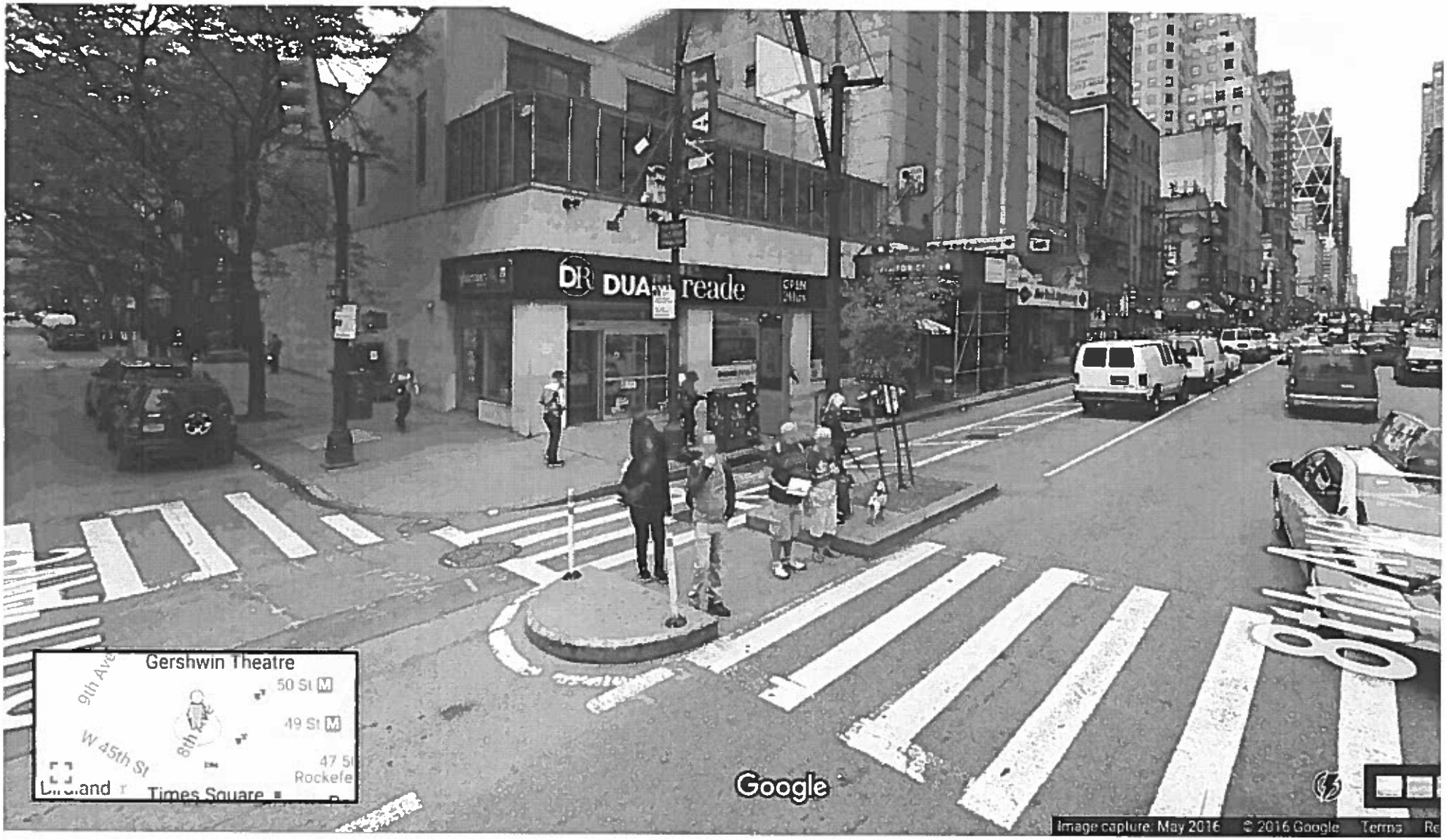
Forensic Computer Expert

Subpoena a Witness from Social Media Provider?

- In person custodian of records
-
- Federal Stored Communications Act
  - 18 USC Sec. 2701

  - self-authenticating certification




DR
reade
OPEN
Gershwin Theatre
9th Ave
50 St M
49 St M
W 45th St
8th
47 5
Rockefe
Times Square
Google
Image capture: May 2016
© 2016 Google
Terms

Google Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043

Google

google-legal-support@google.com
www.google.com

September 12, 2016

Via Email and Express Courier
chris glass55@gmail.com

Christopher M. Glass
Law Offices of Rappaport, Glass, Levine & Zullo, LLP
1355 Motor Parkway
Islandia, New York 11749
631-293-2300

Re: [redacted] **Supreme Court of the State of New York, County of Suffolk, 10722/14 (Internal Ref. No. 780736)**

Dear Christopher M. Glass:

Google Inc. ("Google") has received your subpoena for documents, dated August 24, 2016, in the above-referenced matter seeking documents related to the Street View imagery for ROADWAY ON SOUTH FULTON AVENUE IN THE AREA OF 298 SOUTH FULTON AVENUE.

Google objects to the subpoena on the grounds that it was improperly served. Google is unable to accept service via regular mail, fax or e-mail.

Street View images are publicly available on the Internet. A records custodian from Google is not necessary to authenticate web pages, maps or other such information. Any person may download an image from the Internet and authenticate it for admission. *See, e.g., United States v. Espinal-Almeida*, 699 F.3d 588, 609 (1st Cir. 2012) (allowing Customs officer to authenticate GPS data analyzed using Google Earth, noting that the Rules of Evidence do not require the proponent to "rule out all possibilities inconsistent with authenticity, rather 'the standard for authentication, and hence for admissibility, is one of reasonable likelihood.'") (quoting *United States v. Savarese*, 686 F.3d 1, 11 (1st Cir. 2012). Accordingly, Google objects to the subpoena because it seeks information that is already available from a party to the case.

Street View images viewed in a browser display the month and the year on or about which they were taken in the top left corner of the screen.

Google reserves the right to further object to the subpoena in any additional response.

Without waiving and subject to the below objections, given the limited information provided in the subpoena, Google is unable to determine whether there is relevant data in our records. Google is unable to accurately search its databases by address or by content of the image.

Google objects to the subpoena because it was issued by a state court without subpoena power over nonparty Google. Google objects on the grounds that to seek or compel disclosure from a California resident like Google, Petitioner must comply with Cal. Civ. Proc. Code §§ 2029.100, *et seq.* *See also* the Uniform Interstate Depositions and Discovery Act ("UIDDA"). Google is a California resident and documents and information regarding its business are retrievable and will be produced only from its headquarters in Mountain View, California, USA. Google accepts subpoenas issued from Santa Clara Superior Court via personal service on the Google Custodian of Records for Google Inc.

Google Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043

Google

google-legal-support@google.com
www.google.com

at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

Google objects to your request for an appearance dated September 30, 2016, and does not intend to make a witness available on the requested date pursuant to its objections below.

Pursuant to Rule 45 of the Federal Rules of Civil Procedure, and all analogous rules under any applicable state law, Google, which is not a party to the underlying action, responds and objects to the subpoena for an appearance for at least the following reasons.

1. Google objects to the subpoena for an appearance on the grounds that it imposes an undue burden on Google, a non-party. Google also objects to an appearance on the grounds that the information sought can be obtained through less burdensome means, including from the parties to the case.

2. Google objects to the request for an appearance on the grounds that it is vague, overbroad, duplicative, cumulative, unduly burdensome, and oppressive. Google further objects to the extent that the subpoena is abusively drawn and served for the purpose of annoying and harassing Google, a non-party.

Google objects to the requests in the subpoena to the extent they seek information already in a party's possession or available to a party from some other source (including public sources) that is more convenient, less burdensome or less expensive. This means that if you are seeking information from Google that is equally available from a party in the litigation, Google objects to that request on that basis.

Google also objects to the requests to the extent they seek information containing confidential financial, proprietary or trade secret information, or any information subject to a confidentiality agreement or protective order.

Google further objects to the requests to the extent they seek information protected by any privilege, including the attorney-client privilege, work product immunity doctrine, common interest privilege, or any other applicable privilege, immunity, or restriction on discovery. We also object to the requests to the extent that they are irrelevant, overly broad, vague, ambiguous, unlimited in time or scope, fail to identify the information sought with reasonable particularity, or impose an undue burden on Google, including by seeking electronically stored information that is not reasonably accessible to Google. Finally, Google objects to the requests to the extent that they seek information that is not relevant or reasonably likely to lead to the discovery of admissible evidence.

If you have any questions, please feel free to contact the undersigned at the Legal Support Department alias at GOOGLE-LEGAL-SUPPORT@GOOGLE.COM. Additionally, should you wish to seek any judicial relief in connection with this matter, Google requests the opportunity to meet and confer in advance of any such filing. Thank you.

Very truly yours,

Brittany Araujo
Legal Investigations Support

TEMPLATE QUESTIONS

- ADMISSION OF SOCIAL NETWORKING SITE PHOTOGRAPHS
- ADMISSION OF YOUR OWN CLIENT'S WEB PAGE OR MESSAGE
- CROSS OF ADVERSARY WITNESS ON DAMAGING WEB POSTINGS

A **I believe you're referring to my "My Space"...**
Q I'm not-I-no, I'm not referring to anything. I'm just asking you a simple question: if you'd ever expressed or communicated in any way that you wanted your ex-husband, Mr. Embry, to die a slow painful death?
A **I see it right there on your desk.**
Q Okay.
A **It's my "My Space" blog.**
Q Okay, did you say it?
A **I typed it.**
Q Okay. But the answer is, did you say it? I mean is that your communication.
A **I typed it.**
Q Okay. And did you ever express um, or communicate in any way that you wanted to be present and dance the cha-cha around his slow painful death?
A **It's all there in the blog.**
Q Okay. The answer's a simple yes or no. You said it; you've communicated it some way, did you?
A **If you want to put that blog there, I...**
Q I'm just asking you a simple question.

BY [DEFENSE]:

Prior to April 22nd, 2008 had you ever expressed or communicated in any way that you wanted your ex to die a slow painful death?

A **Yes, I did.**
Q Did you ever refer to Mr. Embry or communicate in any way that he was a worthless bag of monkey s..t?
A **Yes.**
Q Did you ever refer to him as dog _____?
A **Yes.**
Q Did you ever refer to him as a worm puke stale crusty moldy inhuman horrible human oxygen sucking moron?
A **Yes.**
Q Did you ever communicate the desire, that because he's older and more stupid than you, he will die way before you do?
A **I believe I said please assure me that it was possible that he would pass before me."**

BY [COURT]:

Ma'am, will ya just answer the question **yes or no**?

Michael Glass, Esq.

Rappaport, Glass, Levine & Zullo, LLP.

October 20, 2016

Mark D. Cohen
New York State Supreme Court
Cromarty Court Complex - 210 Center Drive
Riverhead, New York 11901
(631) 852-2168

Mark D. Cohen is a Judge of the New York State Court of Claims. He serves as an Acting New York State Supreme Court Justice in Suffolk County, New York and is the Supervising Judge of the Superior Criminal Courts for the Tenth Judicial District.

Judge Cohen is a graduate of Columbia College, Columbia University, and the Hofstra University School of Law, where he was a member and editor of the Law Review. Upon graduation from law school, he was an appellate law clerk in Boston, Massachusetts.

Judge Cohen was the Deputy Director and Chief Counsel of the New York State Office of Homeland Security from 2001 to 2006. During that time, he also served as Acting Director for the Office and Assistant Director for its Legal Division.

Judge Cohen was an Assistant District Attorney in the Suffolk County, New York District Attorney's Office from 1976 through 2001 and served as Chief Assistant District Attorney for thirteen years under two elected District Attorneys. He also was Chief of the Office's Appeals Bureau, Deputy Chief of the Special Investigations Unit, and a trial prosecutor in the Felony Trial Bureau. As a prosecutor, Judge Cohen argued more than 200 cases in the Appellate Division, Second Department, more than 20 cases in the New York Court of Appeals and 10 cases in the United States Court of Appeals for the Second Circuit.

Judge Cohen has been an adjunct law professor at the Touro Law Center in Central Islip, New York since 1993. In 2004, Touro named him Distinguished Public Interest Attorney in Residence. In 2009, the law school honored him as its Adjunct Professor of the Year. In 2013, he received Touro's Annual Award "In Recognition of Devoted Service to the Ideals and Purpose of Legal Education," which in the past, had been reserved only for full-time faculty. During that same year, Touro's Moot Court Honors Board presented him with the Annual Hon. George C. Pratt Award In Appellate Advocacy in recognition of his work with the law school's competitive moot court teams. In 2014, and 2015, Judge Cohen was voted Touro's Best Adjunct Professor by the law school's Student Bar Association. Judge Cohen has also been a lecturer at the State University of New York at Stony Brook.

Judge Cohen has spoken extensively to judicial, governmental, bar, professional, academic, civic, and law enforcement organizations across the country and has lectured for or been a member of the faculty of the New York State Judicial Institute, various Judicial Associations, the National College of District Attorneys, the National District Attorneys Association's National Advocacy Center, the New York Prosecutors Training Institute and the Federal Law Enforcement Training Center. He is a past-President and served on the Board of Directors of the Association of Government Attorneys in Capital Litigation, was a member of the Board of Directors of the Suffolk County Criminal Bar Association, and served as a Legislative Secretary and Treasurer for the New York State District Attorneys' Association.

Judge Cohen has received the New York State District Attorneys Association's highest honor, the Frank S. Hogan Award, and is the only non-elected recipient ever given this award. He has also served as an elected village trustee and deputy mayor, and member and deputy chairman of his local planning board. He lives on Long Island with his family.

Suffolk Academy of Law

Electronic Evidence Overview

Hauppauge, New York
October 20, 2016

Judge Mark D. Cohen

Topics

- Discovery Issues
- Spoliation of Electronic Evidence
- General Foundational Requirements for Admissibility of Electronic Evidence
- Best Evidence
- Fax'es
- Email
- Text Messages
- Social Media
  - Facebook
  - Twitter
  - YouTube
- Judicial Notice of Electronic Evidence: Websites
- Audio Recordings
- Video/Surveillance Recordings
- Forensic Experts – Electronic Evidence
- Computer Animation – Demonstrative Evidence
- Tracking Devices and Information

Electronic Evidence: Some Selected Definitions

Electronic Evidence: Any Probative Information Stored or Transmitted in Digital Form That May Used at Trial [Wikipedia]

Social Media:

- Facebook: Online Social Website That Enables Subscribers to Post Content Such as Photos, Status Updates or Shared Links [www.facebook.com/help]
  - Public & Private Sites
  - "Friends"
  - "Deactivated" Sites
- Twitter: Online Social Network That Enables Users to Send and Read Short 140 Character Messages Called "Tweets"
- LinkedIn: Social networking Site for Business Community; Allows Registered Members to Establish and Document Networks of Those They Know and Trust Professionally
- See Wikipedia List of Major Active Social Networking Sites

Cloud Computer: Software Application and Digital Storage That is Accessed on Internet Through a Web Browser or Mobile Application Software With User Data Stored on Servers at Remote Location

Flash-Drives: Portable Electronic Devices Containing Memory That is Used to Store or Transfer Electronic Data to of From a Computer, Etc.

Metadata: Data Embedded Within a File That Describes a File or Directory Which Can Include Locations Where Content is Stored. Email, Headers and Websites Contain Metadata

Encryption: Procedure That Converts Readable Digital Text Into Symbols to Prevent Any But Intended Recipient From Understanding Message

Overarching Principle:

There Are No New or Even Novel Rules of Law That Are Properly Applied in Discovery or Evidentiary Determinations Involving Electronic Evidence.

Long-Standing Precedents in These Areas Are to be Applied.

Discovery in Cases Involving Electronic Evidence

- Court Rule 202.12 – Preliminary Conference: Establish Method and Scope of Any Electronic Discovery, Including But Not Limited To:
  - Identify Relevant Data & Computer Systems Used
  - Redact Privileged Communications
  - Anticipate and Allocate Cost of Data Recovery
  - Develop Retention of Electronic Data and Preservation Plan
  - Identify Persons Responsible for Data Preservation
- Court Rule 202.16(f): For Matrimonial Cases
- "Litigation Hold" Required to Put Opposing Party on Notice of Need to Preserve
- Failure to Preserve = Spoliation Sanctions
- *Pegasus Aviation I, Inc. v. Varig Logistica S.A., 26 N.Y.3d 543, 2015 WL 8676955 2015, NY Slip Op 09187 (12/15/15)[4/2; Pigott, J.]:* Need "Culpable Mental State" For Spoliation Sanctions in Case Involving Loss of Electronic Evidence + Evidence Relevant to Party's Claim or Defense
  - If Evidence Intentionally or Willfully Destroyed, Relevancy Presumed
  - If Evidence Negligently Destroyed, Party Seeking Sanctions Must Show Documents Relevant to Claim or Defense

Carlene Richards v. Hertz Corp., 100 A.D.3d 728 (2nd Dept. 2012)

- Defendant Sought Access to Plaintiff's "Status Reports, Emails, Photographs and Videos" Posted on Private Settings Portion of Plaintiff's Facebook Account in Personal Injury Action
  - Plaintiff Claimed She Could No Longer Play Sports and Suffered Pain in Cold Weather as Result of Accident
  - But Plaintiff Posted Post-Accident Pix Not Blocked By Privacy Settings Showing Her Skiing
- After Plaintiff Refused to Produce This Information, Defendant Moved to Preclude Plaintiff From Offering Proof on Damages and Plaintiff Then Cross-Moved For Protective Order for Facebook Information
  - Lower Court Denied Defendant's Preclusion Motion and Granted Plaintiff's Protective Order Application
- On Appeal: Case Remitted For In Camera Review and New Determination of Protective Order Issue by Trial Court
  - Defendant Made Sufficient Showing Relevant Evidence Reasonably Calculated to Lead to Discovery of Information Bearing on Plaintiff's Claim

Discovery of Social Network Sites [Cont'ed]

- *Gallo v. City of New York, 43 Misc.3d 1235(A) (Sup. Ct. N.Y. Co. 2014)*
  - Plaintiff Required to Provide Discovery of *LinkedIn* Account Re: Communications With Employment Recruiters in Case Involving Fall From Tree in Central Park
  - Court Applied Two-Pronged Test: Is Material Sought "Material and Necessary" + Would Production Result in Violation of Account Holder's Privacy Rights?
  - Defendant's Motion for Access to LinkedIn Communications With Colleagues Re: Self-Assessment of Post-Accident Condition and "All Social Media Sites" Denied
- *Kregg v. Maldonado, 98 A.D.3d 1289 (4th Dept. 2012)*
  - Order Requiring Production of All Social Media Maintained by Plaintiff Motorcyclist in MV Accident Reversed as Overbroad Without Prejudice to "More Narrowly Tailored Disclosure Request"
- See Also, *1 Modern New York Discovery 12:32.60 (2nd ed)* For Excellent Review of NY Cases on This Issue

Schreiber v. Schreiber, 29 Misc.3d 171 (Sup. Ct. Kings Co. 2010)

- Wife's Motion For Order Confiscating or Copying Hard Drive Disk of Husband's Office Computer on Claim of Concealed Income and Assets Denied as Overbroad Where it Sought General and Unrestricted Access to Entirety of Husband's Business
- Leave to Renew Granted With Proposed Discovery Protocol That Would Protect Privileged and Private Material, Provide Provisions For Discovery Referee, and Forensic Computer Expert, Outline Scope and Methodology of File Analysis, Contain Cost Sharing Plan and Provide for Retention of Clone

Discovery of Social Network Sites [Cont'ed]

- *Romano v. Steelcase, Inc., 30 Misc.3d 426 (Sup. Ct. Suffolk Co. 2010)*
  - Plaintiff Required to Provide Defendant With Access to Private Facebook and MySpace Network Accounts to Contradict Claims She Made in Personal Injury Action
- *Imanverdi v. Popovici, DPM, 109 A.D.3d 1179 (4th Dept. 2013)*
  - Trial Court Order Requiring Plaintiffs to Produce Contents of Facebook Account for In Camera Review Affirmed

Is a Defendant in a Personal Injury Action Involving a Fall Off a Horse Entitled to Discovery of "All Photographs Privately Posted by the Plaintiff on Facebook"?

Kelly Forman v. Mark Henkin, 134 A.D.3d 529 (1st Dept. 2015)

- While Riding One of D's Horses in Westhampton, Stirrup Leather Attached to Saddle Broke, Causing P to Fall
  - P Claimed D Negligent: Failing to Properly Prepare Horse For Riding
- D Sought Order Compelling P to Provide Unlimited Authorization to Obtain Records From P's Facebook Account Including "All Photographs, Status Updates and Instant Messages"
  - P "Deactivated" Facebook Account After Accident and After Commencement of Action
- Sup. Ct Granted Motion –P Must Produce All Photos From Her Private Facebook Account:
  - a) Posted Before Accident P Intends to Introduce at Trial;
  - b) Posted After Accident That Don't Depict "Nudity or Romantic Encounters"; and
  - c) Authorizations For Facebook Records Showing Messages With Postings With Time and Date

Kelly Forman v. Mark Henkin, 134 A.D.3d 529 (1st Dept. 2015) [Cont'ed]

- First Dept. Modified
- Per *Richards v. Hertz* [Previously Discussed] and *McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524, 1525 (4th Dept. 2010)*: Need Some "Threshold Showing of Relevancy" to Warrant Disclosure
  - Discovery Standard in Social Media Contexts is "The Same as in All Other Situations" With No "Fishing Expeditions" Permitted Based on ;"Hypothetical" Hope of Finding Information
  - Merely Because Party Has Used Social Media Does Not Make it Discoverable Without More
- P Must Provide D Only With Photos Posted Before or After Accident She Intends to Use at Trial
- In Camera Review Claim Suggested by D Not Reached on Appeal Since Not Presented to Lower Court
- Justice Saxe, Joined by Justice Acosta, Dissented: Due to Ubiquitous Nature of Social Media Maintained by Litigants in Personal Injury Actions Today, Extra Threshold Burden Should Not Be Required, At Least for Public Facebook Postings
  - Private Facebook Postings Should Be Reviewed In Camera
- See Also, *Medina v. City of New York, 2015 N.Y. Lexis 4702 (Sup. Ct. N.Y. Co. 2015)* [Instagram and Facebook Discovery Requests Overbroad]
- *Compare A.D. v. C.A., 50 Misc.3d 180 (Sup. Ct. West Co. 2015)* [Private Facebook Postings Reviewed in Camera in Matrimonial Action For Discovery Production] with *North Babylon Union Free S.D. v. Feeney, 48 Misc.3d 389 (Sup. Ct. Suffolk Co. 2015)* [In Camera Review of Private Facebook Postings Denied on Insufficient Showing]

And Where Can a Litigant Serve a Subpoena For Electronic Records?

- If Out of State Entity and So-Ordered SDT Sought, Need Local Presence in NYS. See C.P.L.R. 3119 [Uniform Interstate Depositions & Discovery].
- If Electronic Records Sought Belong to Party (i.e., Member or Subscriber of Electronic Evidence Generator or Storage Facility) Authorization May Be Required by Custodian. See *A.D. v. C.A., 50 Misc.3d 180 (Sup. Ct. Westch. Co. 2015).*

General Foundations for Admission of Electronic Evidence

- *Per Lorraine v. Markel Amer. Ins. Co, 241 F.R.D. 534 (D. Md. 2007):*
  - Is it Relevant?
  - Is it Authentic? [F.R.Ev. 901]
  - Is it Hearsay and If So, Is There an Exception?
  - Is it The Best Evidence; If Not, Is There Admissible Secondary Evidence?
  - Does Probative Value Substantially Outweigh Unfair Prejudice [F.R.Ev. 403]

Statutes

- CPLR 4518(a): Admissibility of Business Records:
  - An "Electronic Record" of any Business, (Including a Profession, Occupation or Calling of Any Kind") as Defined in Technology Law 302(2) May be Admissible as Long as Business Record Criteria Established:
    - Made in Regular Course of Business
    - Regular Course of Business to Make
    - Made at or about Time or Reasonable Time Thereafter
- Court May Consider "Method or Manner by Which Electronic Record Was Stored or Maintained or Retrieved in Determining Whether the Exhibit is a True and Accurate Representation of Such Electronic Record"

C.P.L.R. 4539

Copies of Records Made in "Regular Course of Business, Institution or Member of a Professional Calling" Are Admissible If Original is in Existence and Available For Inspection Under Direction of Court

Also, Keep in Mind, F.R.Ev. 901(b)(4)

- Evidence (e.g., Electronic in Nature) May Be Authenticated By Reference to its "Appearance, Contents, Internal Patterns, or Other Distinctive Characteristics, When Taken in Conjunction With The Circumstances"

So, If These Electronic Records Records Are Admissible as Business Records, What About The Best Evidence Rule?

People v. Walter Rath, 41 Misc.3d 869 (Dist. Ct. Nassau Co. 2013)

- State Police Breathalyzer Calibration and Maintenance Records Introduced at Defendant's DWI Trial
- Defendant Convicted and Moved To Set Aside Verdict
- Court Denied Motion and Held: Records Properly Admitted Under C.P.L.R. 4518(a) and STL 302, 304, 305
  - "Electronic Record" Presented as Tangible Exhibit (i.e., Hard Copy) Was True and Accurate Representation
  - Proper Business Record Foundation Laid
- Court Rejected People's Additional Claim They Were Admissible Under C.P.L.R. 4539 Since They Were Never "Stored" or Existed as a "Paper Document" in State Police Records

And What About Fax'ed Documents?

People v. James R. Miller, 199 A.D.2d 692 (3rd Dept. 1993)

- Fax'ed D.C.J.S. Breathalyzer Operator Certification Certificate Introduced in Evidence at Defendant's DWI Trial
- 3rd Dept. Affirmed Conviction and Applied Traditional Best Evidence Rule re: Certificate
- Properly Admitted as Business Record Under C.P.L.R. 4518 Since a "Proper Excuse Was Offered For the Nonproduction of the Original Certificate"
- See Richardson, *Evidence*, Sec. 582 at 589 [Prince 10th ed] and Imwinkelreid, *Evidentiary Foundations*, Sec. 4.03(3), at 68-73

And is an "E-Notarized" Document Admissible?

- L. Prevost, *"E-Notaries Slow to Catch On,"* New York Times 5/25/15, Real Estate @ p. 7
- Short Answer is Admissible Per 2012 Statute in Only Virginia
- Signors Must Appear Before Notary by Live Two-Way Video Conference Which is Recorded – Electronic Signatures Affixed

So How Are E-Mails/Text Messages Authenticated?

- Testimony by "Persons With Knowledge"
  - Sender and/or Recipient
- "Distinctive Characteristics" [i.e., Headers]
  - *U.S. v. Safavian, 644 F. Supp. 2d 1 (D.D.C.2009))*
  - *U.S. v. Kwame Kilpatrick, 2012 WL 3236727 (E.D. Mich. 2012) [NOR]* [Text Messages]
- E-Mail Thread – Context
  - *U.S. v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000)*
- Authentication by Comparison to E-Mails Previously Admitted
  - *U.S. v. Safavian, 435 F. Supp. 2d 36 (D. C.C. 2006)*
- Authentication by Discovery Production
- "Reply Letter" Doctrine
- Authentication by Content
  - *Smith v. Charles, 37 Misc.3d 1229(A) (Sup. Ct. Kings Co. 2012)* - Only Sender Would Have Had Specific Knowledge
- Authentication by Actions Consistent With Message
  - Circumstantial Confirmation

United States v. David Safavian, 435 F.Supp.2d 36 (D.D.C. 2009)

- In False Statements and/or Concealment Trial, Trial Court Granted Government's Application to Admit @260 Emails Under F.R.Ev. 901(b)(4)
- Most Emails Properly Authenticated With "Distinctive Characteristics"
  - Email Addresses: "abramoff@gtlaw.com," DavidSafavian@mail.house.gov and MerrittDC@aol.com (D's Business - Merrit Strategies, LLC
  - Signature Blocks Reflect "To" and "From"
- Court Declined Gov't Request to Admit as Self-Authenticating Under F.R. Ev. 902
- Hearsay and Co-Conspirator Exceptions Addressed

United States v. Mohamed Siddiqui, 235 F.3d 1318, 1322-1323 (11th Cir. 2000)

- In False Statements and Obstruction Prosecution Involving Fraudulent Federal Grant, D.Ct Admitted Inculpatory Emails Between D and Two Sponsors
  - Defendant Maintained Not Sufficiently Established as Authentic
- Held: Per F.R.Ev. 901(b)(4) - They Were Properly Admitted Due to Context and Circumstances:
  - The Emails Had Defendant's Email Address at So. Alabama University
    - Both Sponsors Indicated They Replied to Defendant at This Address
    - Several Made References to Previous Interactions With Defendant
  - Defendant's Emails Referred to Self As "Mo" – Identified by Sponsors as His Nickname
  - Both Sponsors Indicated They Received Telephone Calls From Defendant About Same Subject

General Methods of Proof

- Witness Recognize E-Mail/Text Message Address or Phone Number of Recipient

- Witness Composed E-Mail/Text Message and Pressed "Send" From Witness' E-Mail Address/Telephone Number to Recipient's Address/Telephone Number or Received E-Mail/Text Message From Known Address/Telephone Number

  – *People v. Richard Agudelo, 96 A.D.3d 611 (1st Dept. 2012):* Testimony From Grand Larceny Victim That She Sent and Received Text Messages From Defendant During Alleged Criminal Transaction and Then Compiled Them Into Single "Copy and Paste" Document Held Sufficient

    - Additionally, Detective Testified He Saw Them on Victim's Phone and No Dispute Defendant and Victim Interacted

General Methods of Proof (Cont'ed)

- Outline "Header" Information
  - Actual Receipt of E-Mail is Often Issue

Prove By Technical/Cryptography/Internet Service Provider Evidence

- *People v. Hughes, 114 A.D.3d 1021, 1023 (3rd Dept. 2014)*
- Imwinkelreid, *"Evidentiary Foundations,:"* 8th Ed., Sec. 4.03[4]b at pp.81-102
- Reply Letter Doctrine – Circumstantial Context
- Prove By Content
- Prove by Action Consistent With Message

People v. Marcus Green, 107 A.D.3d 915 (2nd Dept. 2013)

- CW at D's Burglary, Rape and Unlawful Imprisonment Trial Testified Text Messages Purportedly Sent By D And Retained on Her Phone:
  - Were "Actual Photographs of the Screen of [Her] Telephone"
  - That She Saw Detective Taking The Photographs
- In Context, They "Made No Sense Unless … Sent By Defendant"
- Sufficient Evidentiary Foundation Per 2nd Dept.

People v. Emmanuel Pierre, 41 A.D.3d 289 (1st Dept. 2007)

- Trial Court Properly Allowed Testimony From Murder Defendant's Accomplice That Defendant Sent His Cousin an IM In Which He Stated He Did Not Want Victim's Baby
  - Admitted as Admission
  - Accomplice Testified to Defendant's Screen Name
  - Cousin Testified She Sent Defendant an IM to This Screen Name and Received a Reply, Which Made No Sense Unless Sent By Defendant
- IM Not Saved or Printed and No Service Provider or Other Technical Evidence Provided

People v. Al A. Givans, 45 A.D.3d 1460 (4th Dept. 2007)

- Trial Court Admission of a Text Message From Cell Phone in Narcotics Possession Case Held Error Where People Failed to Establish That The Text Was Ever Read By The Defendant or Even Retrieved by Him, Where Insufficient Proof of "Authenticity or Reliability" of Message, Held Error in Dictum
- Case Reversed Due to Jury Selection Error

So, Can an Email With an Electronic Signature Be Used as a Supporting Deposition to Convert a Misdemeanor Complaint into a Misdemeanor Information?

People v. Gustalvo Perez Sanchez, 47 Misc.3d 612 (Cr. Ct. Queens Co. 2015)

- After Arraignment on Criminal Complaint Charging Assault, EWC and Harassment, People Handed up CW's Electronic Signature, Emails Indicating Communications Between CW and ADA [One Indicated CW: "I Agree" With Statements in Accusatory Instrument] and ADA Supporting Deposition to Convert Accusatory Instrument to Misdemeanor Information
- Defendant Claimed No Authority to Accept Electronic Signature and Information Deficient Per C.P.L. 100.40 and *P v. Alejandro, 70 N.Y.2d 133 (1987)*
- Court Held Signature With Supporting Emails Satisfactorily Complied With Statute and Granted People's Motion to Convert The Misdemeanor Complaint to a Misdemeanor Information
- *"Not Only Was the Complainant Provided With the Language of the Complaint and Its Allegations, The District Attorney's Email Also Provided a Very Clear, Unambiguous Explanation of What the Legal Effect of Typing Her Name in a Response Email; Would Be"*
- Ruling Consistent With Clear Legislative Policy to Promote Use of Electronic Signatures to "Facilitate Business as Well as the Business of New York State."
- See Also, *People v. Robinson, __Misc.3d __ (Cr. Ct. Kings Co. 2016), N.Y.L.J. 3/18/16 @ p. 21* [Same Holding Relying on Tech Law 304(2)]

Social Media

- No New or Distinctive Evidentiary Rules For This Electronic Evidence
  - Authenticity is Usual Issue
- Per *People v. McGee, 49 N.Y.2d 48 (1979)* – Need Proof Evidence is Genuine and No Tampering
- Per *Griffin v. State, 419 Md. 343, 364-365, 19 A.3d 415, 227-428 (2011)* Three Non-Exclusive Methods:
  - Did Purported Creator Create Profile and Post Content in Question?
  - Can Search of Person's Computer Determine Computer Used to Create Posting?
  - Can Profile and/or Postings Be Linked to Person Who Purportedly Created Posting?

So, Can a Person Be Charged With Criminal Contempt Based on Allegations that She Communicated With a Protected Party on Facebook in Violation of an Order of Protection?

People v. Maria Gonzalez, (Co. Ct. Westchester Co. 2016), N.Y.L.J. 1/15/16 @ p. 21 [N.O.R.]

- Yes – Especially If the Order of Protection Has Language That Specifically Proscribes Communication With Protected Party by "Electronic Means."
- Indictment That Charged Criminal Contempt Based on These Allegations Valid – Motion to Dismiss Denied
- See Also, *People v. Thomas Horton, 24 N.Y.3d 985 (2014)* [Posting of Undercover Police Surveillance Recording of Narcotics Transaction on YouTube to "Out" Informant, Witness Tampering]

And Can an Action be Commenced by Service of a Summons Through a Facebook Account?

- Yes
- *Baidoo v. Blood-Dzraku, 2015 NY Misc. Lexis 977 (Sup. Ct. N.Y. Co. 2015):* Service, in Divorce Action, "While Novel," Permitted After Efforts At Regular Service Failed by Sending Summons Through Private Message Through Facebook Account Three Consecutive Weeks
- DRL 232 and CPLR 308(5) Permits Alternative Methods of Service
  - Proof Submitted: Wife Communicated With Husband Though Facebook Account, Husband Regularly Logs Into Account

What if There is Proof That the D's Email Address Critical to the Transfer of an Alleged Fraudulent Document is Associated With a Foreign Facebook-Like Account He Maintains?

- Is That a Sufficient Foundation to Permit Proof From the Account in Evidence?

United States v. Aleksander Zhyltsou, 769 F.3d 125 (2nd Cir. 2014)

- D Charged in E.D.N.Y. on Single Charge of Transfer of a False ID Document
  - Forged Birth Certificate of Invented Infant Daughter as "Favor" to Enable Friend to Defer Army Service in Ukraine
    - Certificate Created While Two Sat in Internet Bklyn Internet Café
- Friend Did Get Deferment Based on Forged Certificate
- Gov't Offered into Evidence Printed Copy of D's Russian Social Networking Site, "VK"
  - Proof of Emails on Gmail Account D Sent Forged Certificate From New York to Friend
  - Spec Ag of U.S. DOS Diplomatic Security Service Testified:
    - "VK" Website Was "Equivalent to Facebook" and Discussed Profile Page, Which Witness Said Had D's Name on it and Same Gmail Address
    - Had Only "Cursory Familiarity" With "VK" and Not Aware of What Identity Verification Was Required to Create Account
- D.Ct. However, Concluded That it Was Fair to Assume Information on Website Provided by the D

United States v. Aleksander Zhyltsou, 769 F.3d 125 (2nd Cir. 2014)

- 2nd Circuit Reversed D's Conviction
  - Insufficient Proof of Authentication and That Document Was Indeed Created by D as Required by F.R.Ev. 902
- Document Not Self-Authenticating Under F.R.Ev 901 and 902, Since There Was Insufficient Proof Document Was What Proponent Government Said it Was
- Court Does Not Reach Dicta in *Griffin v. State (Md. 2011)* [Evidence Derived From Internet Must Be Reviewed on Admissibility With "Heightened Scrutiny"
- See Also *Smith v. State, 136 So.3d 424 (Miss. 2014):* Similar Holding in FaceBook Account Posting Case
- Excellent Discussion of Case: M. Hutter, "*Admissibility of Evidence Obtained From Facebook*," N.Y.L.J. 4/7/16 @ p. 3.

Ronnie Tienda v. State of Texas, 358 S.W.3d 633 (Tex. Crim. App. 2012)

- 3 MySpace Accounts Admitted in Evidence During Guilt and Penalty Phases in Texas Gang Capital Murder Case
  - Shooting Between Rival Gangs on Interstate in Dallas
- Profile Pages Contained D's Purported Boasts
  - "You anit BLASTIN You aint Lastin" & "I Live to Stay Fresh!! I Kill to Stay Rich!!"
  - Another Link: "I Still Kill"
  - IM's Exchanged Between Account Holder Included Specific References to Other Passengers Present During Shooting and Police Investigation
    - "WUT GOES AROUND COMES AROUND" & "U KNO HOW We DO, We DON"T CHASE EM We REPLACE EM"
- Per Subscriber Reports, 2 Profiles Created by "Mr. Ron T." and One by Smiley Face" (D's "Widely Known Nickname")
- Expert Gang Unit PO Testimony: Gangs Use Social Media to Communicate and Threaten

Ronnie Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012)

- D's Conviction Affirmed: State Properly Presented Prima Facie Case to Authenticate MySpace Postings, Per *Griffin v. Maryland (2011)* With Sufficient Circumstantial Evidence That They Were Created by Defendant Based On:
  - Numerous Photos of D With Unique Arm, Body & Neck Tattoos
  - Particular References to V's Death and Music at His Funeral
  - References to D's Gang
  - Messages Regarding Shooting
  - References to D Wearing Ankle Bracelet Monitor
- See Also *Parker v. State, 85 A.3d 682 (Del. 2014):* Similar Holding – Post on Facebook Page Sufficiently Authenticated in Assault Case Based on Distinguishing Characteristics

Reliability of Purported Posted Communication and Connecting Party in Question With Posting Is Generally The Pivotal Issue

Antoine Levar Griffin v. State, 419 Md. 343, 19 A.3d 415 (2011)

- Trial Court Admitted Screen Shots of Several Pages of Murder Defendant's (aka "Boozy") Girlfriend's MySpace Profile
- Permitted Evidence Through Testimony of Police Investigator Who Accessed Site to Demonstrate Prior to Trial Girlfriend Threatened Another Witness Called by State
  - Profile: "Sistasouljah," "23 Year Old Female," From "Port Deposit Maryland," With DOB: "10/02/1983"
  - "FREE BOOZY!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!
- Because Anyone Can Create MySpace Profile, Majority Held Identity of Creator Not Reliably Established or Authenticated to Meet Fabrication Concerns and Conviction Reversed
  - Emails. IM's and Text Messages Issues Differ "Significantly" Since Correspondence is Sent Directly From One Party to Another, Rather Than Published for All to See
  - Dissenters: "Technological Heebie-Jeebies" Aside, Sufficiently Authenticated
- See Also, *People v. Albert Sublet IV,, 2015 WL 1826582 (Md. 4/23/15)* [Extensive Review of Admissibility Requirements for Facebook, Twitter (Direct Messages and Public Tweets), and Facebook Messages]

People v. Richard Clevenstine, 68 A.D.3d 1448 (3rd Dept. 2009)

- Computer Disk Containing Electronic Communications Between Sex Crime Victims and Defendant Via IM's Held Properly Authenticated and Admitted in Evidence
- Two Victims Testified The IM'ed Defendant About Sexual Relations on MySpace Account
- State Police Investigator Testified He Retrieved Such Conversations From Hard Drive of One of Victim's Computers
- MySpace Legal Compliance Officer Testified That Messages on Computer Disk Had Been Exchanged by Users of Accounts Created By Defendant
- Defendant's Wife Testified She Viewed Sexually Explicit Communications on Defendant's MySpace Account

People v. Karon Lenihan, 30 Misc.3d 289 (Sup. Ct. N.Y. Co. 2010)

- Trial Court Precluded Murder Defendant From Confronting People's Witnesses About Gang Affiliation About Gang Affiliation Based on MySpace Photographs
- Court Held Ability to "Photoshop," Edit and Otherwise Manipulate Photographs Precluded Authentication of Postings
  - Defense Counsel's Good Faith Basis to XE Also Rejected
- Cited With Approval By *Griffin* Majority
- See Also, *People v. Robert Johnson, 2015 N.Y. Misc. Lexis 4744 (Co. Ct. Sullivan Co. 12/31/15)* [Purported Facebook Materials of Victim in Predatory Sexual Assault Case Not Properly Authenticated]
- 120 Am Jur Proof of Facts 3rd 93, M.C.M. Leahy, *"Pretrial, Involving Skype, YouTube and Other Video Electronic Communications"*

Investigators Download a You-Tube Video From the Internet Showing the Defendant Shooting Off an AR-15 Rifle at a Firearms Dealer in a Prosecution For Being in Possession in Possession of a Firearm.

The Prosecution Seeks to Introduce It In Evidence With Foundational Proof That The Investigator Downloaded the Video and Recognized the Defendant From Previous Encounters and That the Firearms Dealer Recognized Weapon as One Sold by Him at Certain Time and His Establishment's Shooting Range in the Video.

Do You Admit It or Not?

United States v. James Franklin Broomfield, 591 Fed Appx. 847 (11th Cir. 2014)

- Admit it – Conviction Affirmed
- The You-Tube Video Was Properly Authenticated
  - Prosecution Established D in Video in Possession of Firearm
- Ordinary Foundational Proof That Video Equipment Was Working Properly Does Not Apply Where Prosecution Found Video on the Internet, Where There Was "Substantial Evidence" Where and When Video Was Made and Who Was Depicted In It

And, Of Course, The Social Media Proof Must Be Probative.

- *People v. Jule Frazier, 2015 NY Slip Op 03561 (2nd Dept. 4/29/15)* [Photos Posted by D in Weapons Trial Properly Admitted Where They "Tended to Prove Material Issues," "Illustrate[d] or Elucidate[d] Other Relevant Evidence," and Probative Value Outweighed Prejudice]
- *United States v. Pierce, 2015 U.S. App. Lexis 7717 (2nd Cir. 5/11/15), N.Y.L.J. 5/12/15 @ p. 1* [Facebook Posts Containing Rap Video and Tattoos Properly Admitted in Drug and Gang Murder Prosecution; "Freedom of Expression" Claim Rejected; Probative Value Also Held Outweighed Prejudice]

Some Exceptions to Hearsay: Electronic Evidence

- Admission of Party-Opponent
  - *Sea-Land Serv., Inc v. Lozen Int'l, LLC, 285 F.3d 808 (9th Cir. 2002):* Email Forwarded by Party-Opponent:
- Business Records: CPLR 4518
  - Computer Printouts
  - Medical Records – Treatment and Diagnosis
- State of Mind:
  - Effect of Emails on Plaintiff's State of Mind in Libel Action: *Rombom v. Weberman, 2002 WL 1461890 (Sup Ct. Kings Co. 2002), aff'd, 309 A.D.2d 844 (2nd Dept. 2004)*
- NY Common Law Public Records Exception:
  - *Miriam Osborn Memorial Home Assoc. v. Assessor of City of Rye, 9 Misc.3d 1019 (Sup. Ct. Westch. Co. 2005)* – Printout of Webpage of Gov't Website Containing Real Property Sales Information Admissible
- CPLR 4539: As Discussed, Copies of Records Made in "Regular Course of Business, Institution or Member of a Professional Calling" Are Admissible If Original is in Existence and Available For Inspection Under Direction of Court

Palisades Collection LLC v. Barbara Kedik, 67 A.D.3d 1329 (4th Dept. 2009)

- Plaintiff, as Claimed Assignee of Defendant's Credit Card Debt Submitted Affidavit From Discover Bank With Attached Spreadsheet Listing Defendant's Discover Account as Debt Sold to Plaintiff in Support of Action to Recover Balance Owed on Card
- Court Affirmed Lower Court Order Dismissing Lawsuit on Plaintiff's Standing to Sue
  - Although Plaintiff's Purported Agent Averred Spreadsheet Was Kept in Regular Course of Business and Entries Therein Made in Regular Course of Business, Agent Failed to Establish "When, How or By Whom The Electronic Spreadsheet Submitted in Paper Form Was Made" or That He Was Familiar With Discover's Business Practices or Procedures

People v. Daniel Manges, 67 A.D.3d 1328 (4th Dept. 2009)

- Trial Court Erred in Admitting Printout of Electronic Data That Was Displayed on Computer Screen as Business Record as Proof Defendant Presented a Check Claimed to Be Forged
- No Proof Data Resulting in Printout Entered in Regular Course of Business of Bank
- Indeed, Bank Teller Testified, "Anyone [At The Bank] Can Sit Down at a Computer and Enter Information"

The Court Issues 381 Digital Search Warrants That Seek All User Information From Facebook“ Comprising Every Posting and Action” Taken by Each of The 381 Facebook Users.

Can Facebook Challenge the Constitutionality of These “Bulk Warrants” Pre-Enforcement?

Or Does it Have to Wait Until The Warrants Are Executed and Defendants Are Charged?

Or Can They Litigate Privacy Interests “*Ex Ante*” by a “Motion to Quash”?

In Re 381 Search Warrants Directed to Facebook, 2015 N.Y. App. Div. Lexis 6067 (2nd Dept. 2015)

- 2nd Dept (Renwick, J.) Affirmed Supreme Court Order 4-0 Summarily Dismissing Pre-Enforcement "Motion to Quash" the Search Warrants
- No Constitutional or C.P.L. Right to Contest Efficacy of SW Pre-Execution ["Ex Ante"]
- Thus, No Corollary to Civil Motion to Quash in Search Warrant Setting Under Constitution or C.P.L. Even to Contest Privacy Rights
- Additionally, No Right Afforded Facebook to Contest Pre-Execution Under Stored Communications Act, 18 U.S.C. 2703(d)
- Leave Has Been Granted to the Court of Appeals [26 N.Y.3d 914 (2015)]
- And FYI: In In re: *Grand Jury Subpoena to Facebook [#16-mc-1300], N.Y.L.J. 5/16/16 @ p. 1,* E.D.N.Y. Magistrate Judge Orenstein Questioned "Boilerplate" Non-Disclosure Orders on Gov't SDT and Required Greater Specificity

Judicial Notice of Electronic/Website Evidence

- Government Examples
  - Court of Record's Computerized Records
  - Official Government Websites [F.R.Ev. 902(5) – Self Authenticating]
    - Downloading Information – Hearsay Issues vs. Inherent Reliability
  - NYS DOS – "Entity Information"
  - N.Y.S. DOS – Professional Licensing Information
  - U.S. Naval Observatory – Time of Sunrise
  - Federal Reserve Board – Prime Interest Rate
  - National Personnel Records Center – Retired Military Personnel
- Private – Commercial Examples
  - *Mapquest* for Driving Distances
  - Hospital Websites for Medical Conditions and Causes *[Gallegos v. Elite Model Management Corp. 195 Misc.2d 223 (Sup. Ct. N.Y. Co. 2003), aff'ed as modified, 28 A.D.3d 50 (1st Dept. 2005)]*
  - Retirement Earnings Posted on Website [*O'Toole v. Northup Grumman Corp., 499 F.3d 1218 (10th Cir. 2007)*] – T.Ct. Erred in Not Taking Such Judicial Notice

N.Y.C. Medical and Neurodiagnostic, P.C. v. Republic Western Ins. Co., 3 Misc.3d 925 (Civ. Ct. Queens Co., N.Y. 2004)

- Trial Judge Made Independent Review of Website to Determine if Doing Business in NY
- On Motion to Renew, Court Held That Even Assuming It Took Judicial Notice of Facts - Information Posted on Corporate Party's Website Constitute Admissions and Are Encompassed by Admissions Exception to Hearsay
- But On Appeal [8 Misc.3d 33 (App. Term 2004)] – Reversed: No Showing Website Was of "Undisputed Reliability" & Opposing Party Had No Opportunity to Be Heard

Tape/Digital Recordings

- Witness Qualified to Operate Recording Instrument
- Witness Recorded a Certain Conversation
- Witness Used Certain Equipment to Record
- Equipment Was in Good Working Order
- Proper Procedures Were Used to Record
- Chain of Custody Maintained Over Tape/CD
- Witness Listened to Tape/CD Recording and It is Fair and Accurate Reproduction/Depiction of Conversation
- Witness Recognizes Tape/CD as the Same as One Used
- Transcript is Helpful but Only as Aid to Jury/Court

So, What About Tape-Recorded Conversations Between a Murder Victim and the Defendant That Were Purportedly Recorded by Victim at an Unknown Time and Placed in Storage Before Being Provided by Roommate to Police?

Have These Been Properly Authenticated?

People v. Karen T. Ely, 68 N.Y.2d 520 (1986)

- DA Sought Admission in Evidence of Tape Recorded Conversations Between D and V, Her Husband, in Murder by Strangulation Case
  - DA Claimed Motive For Murder Was to Prevent V From Exercising Overnight Parenting Time as Part of Pending Divorce Case in Albany
- Tapes Admitted on This Foundation:
  - Two Tapes: V's Roommate Testified: V Made Them at an Unknown Time and Place; Stored It in Their Home and After Murder, Turned it Over to Police
  - Third Tape: V's Matrimonial Lawyer Testified V Gave it To Him After "About 3-4 Weeks," There Were Notations On It In V's Handwriting

People v. Karen T. Ely, 68 N.Y.2d 520 (1986)

- Court of Appeals Reversed 7-0
- Foundation For Admission of Tape Recordings is "Clear and Convincing Proof That the Tapes are Genuine and That They Have Not Been Altered"
- Court Outlined 4 Methods For Proper Foundation:
  - 1) Testimony of a Participant in the Conversation that it is a "Complete and Accurate Reproduction of the Conversation and Has Not Been Altered;
  - 2) Testimony of a Witness to the Conversation or its Recording (Such as the "Machine Operator" to the Same Effect;
  - 3) Testimony of a Participant in the Conversation Together with Proof by an Expert Witness after Analysis "Of the Tapes for Splices or Alterations"; or
  - 4) Demonstration of a "Chain of Custody" that Establishes, in Addition to Evidence Concerning the Making of the Tapes and Identification of the Speakers, That Within Reasonable Limits, Those Who Handled Tape from its Making to its Production in Court Identify it and Testify to its Custody and Unchanged Condition.
- Method # 4 Employed Here Insufficient

People v. Mathew P. Galunas, 107 A.D.3d 1034 (3rd Dept. 2013)

- People Offered Tape-Recorded Conversations Between D and CI in Narcotics Task Force Investigation
- Foundation Proper: Per *People v. Ely* on "Clear and Convincing" Proof:
  - Detectives Testified to "Events Surrounding Creation of Recordings, Indentified the Voices of the Informant and Defendant and Set Forth a Chain of Custody of the Recordings"
    - Detective-Operator of Recorder Immediately Reviewed Recording at Conclusion of Conversations, Secured Them In Police Custody, Immediately Prior to Trial Reviewed Recordings and Confirmed They Were "Fair and Accurate."
    - A Second Detective Testified That He Knew D for 35 Years and Identified One Voice on the Recording as the D's

People v. Randy Dicks, 100 A.D.3d 528 (1st Dept. 2012)

- At Narcotics Sale Trial Foundation for Admission of Tape-Recorded Conversations Established By:
  - Testifying Detectives (i) Described Creation of Recordings and (ii) Identified Voices of Informant and D on Recordings
- Defendant's Identity as Speaker on Recording Established by Testimony of Another Participant in Conversation, as Well as Surrounding Circumstances, Including Several Face-to-Face Meetings
- See Also, *People v. Jackson, 121 A.D.3d 1185 (3rd Dept. 2014)* [Same Holding in Controlled Buy Narco Case]

What About Jailhouse Recordings?

Are They Admissible in a Criminal Trial Is The Recordings Are Made Pursuant to Correctional Facility Regulations?

People v. Marcellus Johnson
27 N.Y.3d 169 (2016)

- Excerpts of Telephone Calls Made by NYC Rikers Island Pre-Trial Detainee Admitted at Robbery Trial
- Recorded Per NYC Regulations and Obtained by People's SDT
- Per Court of Appeals 7-0 (Rivera, J.), They Are Admissible Where There is No Violation of the Attorney-Client Relationship
- Court Rejected Claims That Recording Program Exceeded Scope of Corrections Department Regulatory Needs

What About Surveillance Recordings?

People v. Darren Patterson, 93 N.Y.2d 80 (1999)

- Same Rules For Admission of Video Surveillance Recordings as For Audio Recordings
  - Need Proof of Authentication and Foundation, Including Chain of Custody to Demonstrate Integrity
- Court Reversed Conviction on Other Grounds But in Dictum Held Admission of Commercial Store Surveillance Recording of Robbery Error:
  - Proof "Too Tenuous and Amorphous"
  - 911 Call Apparently Recorded Background Noises of Unidentified Man Reporting Robbery Insufficient to Provide "Inferential Linkages"

People v. William Hill, 110 A.D.3d 410 (1st Dept. 2013)

- "Common Sense" Approach Adopted to Permit Admission into Evidence of Surveillance Video Based on Testimony of Moonlighting Detective Who Stated That While Working Second Job For Security Company, Hooked Up the Surveillance Cameras to the Video Recorder and Checked on a Daily Basis That The System Was Functioning Properly
- Detective Also Testified to Unaltered Condition of Tape = Trial Court Properly Concluded Video Accurately and Completely Depicted The Events at Issue

People v. Philip J. Messina, 43 Misc.3d 78 (App. Term 2nd Dept. 2014)

- Copy of DVD Surveillance Recording Introduced in Evidence Over Objection in D's Bench Contempt Trial
  - DVD Purportedly Captured Images of D Throwing Hammer at Home of D's Former BIL and SIL Who Were Protected by TOP
  - SIL Copied DVD and After Providing it to Investigator, Over-Written Within 48 Hours of Copying
    - Testified to Installation and Manner Surveillance Equipment Maintained
  - D's Estranged W Testified She Witnessed Entire Incident
- D's Request For Adverse Inference Instruction Re; Uncopied Portion Denied

People v. Philip J. Messina, 43 Misc.3d 78 (App. Term 2nd Dept. 2014)

- App. Term Affirmed
- Video Properly Authenticated by W's Who Knew Instrument and D
  - D Had Every Opportunity to Submit DVD to Expert to Challenge its Authenticity and Did Not
- D's Claim Tape "Faked" Rejected Even With Short Gaps in Recording
  - People Had No Control Until DVD Copy Provided to Investigator
- Adverse Inference Request Properly Denied (Again it Was a NJ Trial) & If Error Harmless Due to EW Evidence
- Also No *Brady* Error Either Since Per *P v. Hayes, 17 N.Y.3d 46 (2011),* No Affirmative Duty by Police to Collect Exculpatory Evidence

A Surveillance Tape of a Portion of Jailhouse Altercations Between an Inmate and Another Inmate and Sheriff is Inadvertently Taped Over and Lost After The Defense Requested It Be Produced.

Is The Defendant Entitled to an Adverse Inference Charge?

People v. Dayshawn P. Handy, 20 N.Y.3d 663 (2013)

- D Involved in Two Fights in County Jail - Two Months Apart
  - One on Inmate and One on Sheriff
- Surveillance Captured Portions of Area of Incidents
- D Timely Demanded Production of Videos But ….
- Both Were Destroyed Due to Routine Tape Over/Re-Using by Facility Per Jail Policy After 30 Days
- TJ Refused to Provide Adverse Inference Charge on All Charges Per DC Request
  - Issue Whether DC Had Requested Production of Both Incidents
- D Convicted of Only One Incident
  - Adverse Inference Charge Not Provided on This Count
- Court of Appeals Reversed 6-0 (Smith, J.): Holding as a Matter of New York Law of Evidence:
  - *"When a criminal defendant, acting with due diligence, demands evidence that is reasonably likely to be of material importance, and that evidence has been destroyed by the State, the defendant is entitled to a permissive adverse inference instruction charge"*
- Incentive to Avoid Destruction of Evidence and Raise "Consciousness" of State
- New CJI Instruction Per *Handy* Re" Destroyed Evidence

Expert Witness on Electronic Evidence Foundation

- Imwinkelreid, *"Evidentiary Foundations"* 4.03, Sec. 4.10 at pp. 169-204
- 40 A.L.R. 6th 355 "Admissibility of Computer Forensic Testimony"

How About Expert Testimony Re: Cell Site Location?

People v. Darryl Littlejohn, 112 A.D.3d 67 (2nd Dept. 2013)

- Expert Cellular Phone Tracking [Cell-Site] Evidence Held Properly Permitted Without *Frye* Hearing Where Basis of Testimony Rested on Generally Accepted Scientific Processes

Computer Animation?

- Demonstrative Evidence
- Proof: Fair and Accurate Representation + Consistent With Proponent Witness's (Lay or Expert) Testimony or Other Admitted Evidence
- Imwinkelreid, *"Evidentiary Foundations,"* 8th Ed., Sec. 4.09[4]b], at pp.155-173
- See *People v. Morency, 93 A.D.3d 736 (2nd Dept. 2012)* [Computer Animation Illustrating Expert's Testimony Re: Shooting of V Properly Admitted]

Mathew Kane v. TBTA, 8 A.D.3d 239 (2nd Dept. 2004)

- In MVA Case on Marine Parkway-Gil Hodges Bridge, T Ct. Properly Admitted Plaintiff's Video of Computer Generated Animation of Accident, Which Included Still Photos, to Re-Enact The Incident and Illustrate Plaintiff's Expert's Opinion Concerning Cause.
- In Affirming 2nd Dept Noted: Whether a Video Re-Creation Should Be Viewed by Jury Depends on "Facts and Circumstances" of Case in The Court's Sound Discretion
  - If There is Any Tendency to Exaggerate What is Sought to be Proved, Court May Reject The Evidence

People v. Gregory Morency, 93 A.D.3d 736 (2nd Dept. 2012)

- Where "Conditions Present in The Computer-Generated Animation Were Sufficiently Similar to the Conditions Present at The Time of The Shooting," in a Manslaughter Case, This Evidence Was Properly Admitted as Demonstrative Proof

Illegally Obtained Recordings

- C.P.L.R 4506: Contents of Illegally Obtained Intercepted Electronic Communications (and Any Derived Evidence) Inadmissible in Any Trial or Hearing
  - Applicable to Both Criminal and Civil

McLaughlin v. McLaughlin, 104 A.D.3d 1315 (4th Dept. 2013)

- Family Court Admitted Audio of Incident in Home Between H and W, Recorded With Either Party's Knowledge on Order of Protection Application
- 4th Dept. Affirmed: The Parties' Son Was Present and Thus Consented to Recording
  - CPLR 4506 and P.L. 250.02 Not Implicated

Gurevich v. Gurevich, 24 Misc.3d 808, (Sup. Ct. N.Y. Co. 2008)

- W Accessed Emails From H's Account Using His Password in Support of Child Support Claims
  - Claimed No Revocation of Permission
- H Claimed They Were "Stolen" and CPLR 4506 Required Suppression
- Court Rejected Claim This Was "Eavesdropping" or Unlawful Accessing of "Electronic Communication" Under P.L. 250.05
- Material Was Not "Intercepted" But "Stored"
  - *Moore v. Moore, N.Y.L.J. 8/14/08 @ p. 26 (Sup. Ct. N.Y. Co)*
  - *Boudakian v. Boudakian, N.Y.L.J. 12/26/08 @ p. 27 (Sup. Ct. Queens Co.)*

The Defendant Lives With His Girlfriend And Her 5 year Old Son. The Child's Father Has Visitation Rights. The Child Cries and Refuses to Return to the Mother's Home. The Mother Calls the Police and the Child is Returned. Shortly Thereafter, The Father Calls the Mother on Her Cellphone. After Several Attempts, The Call Went Through But No One Answered. The Father Could Hear The Defendant Threatening to Beat His Son. The Father Then Recorded The Continued Threats to Beat and Hurt The Child. The Father Does Not Report This to the Police.

Several Months Later, The Defendant's Landlady Hears Screaming and Crying From The Defendant's Apartment.

The Police Respond and Arrest the Defendant.

Is The Recorded Statement Admissible or Is it Barred By CPLR 4506 As an Illegal Recording?

People v. Anthony Badalamenti, 27 N.Y.3d 423 (2016)

- It's Admissible Per Court of Appeals 4-3 (Fahey, J.)
- The Recorded Conversation Between The Defendant and the Child Was Not Illegal Eavesdropping or "Bugging" Under P.L. 250.00(2)
- Per *Pollack v. Pollack, 154 F.3d 601 (6th Cir. 1998),* Father Had Vicarious Consent to Record Son's Conversation With Defendant as Adopted by *People v. Clark, 19 Misc.3d 6 (App.Term)*
- Father Reasonably Believed Necessary to Protect Well-Being of Son Which Had Objective Basis as Well
- But Decision Should Not Be Interpreted as Vehicle For Parent to Act in Bad Faith
  - Courts Should Consider: Parent's Motive of Purpose, The Necessity of the Recording to Serve the Child's Best Interests, The Child's Age and Maturity and The Ability to Formulate Well-Reasoned Judgments on Own

What About E-Z Pass Information?

- Generally Held Admissible:
  - *Gale v. Gale, 2009 WL 2612314 (N.J. Super. 2009)*
  - *S.S.S. v. M.A.G., 2010 WL 4007600 (N.J. Super. 2010)*

G.P.S. Evidence

- Law Enforcement Needs a Probable Cause Warrant/Order to Obtain G.P.S. Evidence
  - *People v. Weaver, 12 N.Y.3d 433 (2009)* [Per NYS Constitution]
  - *United States v. Antoine Jones, 132 S.Ct. 935 (2012)* [Per Fourth Amendment]
- State Attaching G.P.S. Device on Employee's Private Car "Unreasonable"
  - *Matter of Cunningham v. NYS Dept. of Labor, 21 N.Y.3d 515 (2013)*
- What About Private G.P.S./Tracking Devices?
  - Do They Fall Within C.P.L.R. 4506?
  - Or Are They Admissible Because The Evidence Isn't "Eavesdropping" and Are Obtained by Private Actors?

What About Tracking The Location of Cellular Telephones First By Gov't?

- *In re Application For Order For Prospective Cell Site Location Information, (S.D.N.Y. 2006)* When Cell Phone is in "On" Condition, Regardless of Whether It's Making or Receiving Voice or Data Call, It Periodically Transmits Unique ID # to Register Location Within Network
  - Signal Sent to Every Antenna Tower Within Range of Phone – Switching Capability of System Temporarily Assigns Phone as it is Moved to Nearest Tower
    - It Can Be Connected to Two or More Towers at Once, Depending on System & Location (Urban, Suburban or Rural)
  - Location of Tower Receiving Signal From Cell "Generally Fixed" in Real Time
    - Depending on System and Software Employed, By Mathematical Process of "Triangulation," [Two Towers With Cell, 3rd Point] Can Determine Location
    - Another Method is "Pinging" Which Discloses Cell Tower Range Where Cell Phone is Located [See P. Crusco *"Ringing, Pinging and the Fourth Amendment,"* N.Y.L.J. 6/25/13 @ p. 5
- FCC Regulation [47 CFR 20.18(h)(i)]: By 9/11/12, Cell Phone Carriers Required to Have Ability to:
  - Locate Phones Within 100 Meters For 67% of Calls and Within 300 Meters For 95% of Calls For Network-Based Calls
  - Locate Phones Within 50 Meters For 67% of Calls and Within 150 Meters For 95% of Calls For Hand-Set Based Service

The Answer Is…

- Still Undecided by SCOTUS – At Least For Government Action
- PC Not Required: *United States v. Davis, 754 F.3d 1205, opinion vacated and petition for re-hearing en banc granted, 573 Fed. Appx. 925 (11th Cir. 2014); In Re Application of The United States For Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) and United States v. Skinner, 690 F.3d 772 (6th Cir. 2012)* [Need Only "Specific and Articulated Facts" Under Stored Communications Act-18 U.S.C. 2307]
- Other Courts to Contrary: *State v. Earls 70 A.3d 630, 2013 WL 3744221 (Sup. Ct. N.J. 2013)* [Need PC Warrant]
  - On Remand, Ct. Determined "Emergency Aid Exception" Inapplicable: 2014 N.J. Super Unpub..Lexis 238 (2014)
  - See Also, *United States v. Graham,* 2016 U.S. App. Lexis 9797 (4th Cir. 2016) [Warrantless Acquisition of Cell-Site Information Not Violative of 4A], aff'g 796 F.3d 332 (4th Cir. 2015) [Upholding Gathering of Information on Good Faith Exception]
- *People v. Littlejohn, 113 A.D.3d 67 (1st Dept. 2013)* [Expert Cell-Site Evidence Properly Admitted in Murder Case Without *Frye* Hearing]
- SDT's to Phone Companies For Third Party Cell-Site Records?
- " Sting Rays" and "Dirt Boxes" – Cell Site Simulators? See J. Baird, *"Unlocking the Dirtbox: Confronting Cell Phone Location Tracking With the Fourth Amendment,"* 57 Boston College Law Review 731 (2016)

Tape Recordings

- Witness Qualified to Operate Recording Instrument
- Witness Recorded a Certain Conversation
- Witness Used Certain Equipment to Record
- Equipment Was in Good Working Order
- Proper Procedures Were Used to Record
- Chain of Custody Maintained Over Tape/CD
- Witness Listened to Tape Recording and It is Fair and Accurate Reproduction/Depiction of Conversation
- Witness Recognizes Tape/CD as the Same as One Used
- Transcript is Helpful but Only as Aid to Jury

Selected Articles of Interest

- G. P. Joseph, *"What Every Judge and Lawyer Needs to Know About Electronic Evidence: Authentication,"* 99 Judicature, No. 2 (2015)
- M. J. Hutter, *"Admissibility of Evidence Obtained From Facebook,"* N.Y.L.J. 4/7/16 @ p. 3.
- P. A. Crusco, *"Authenticating Digital Evidence,"* N.Y.L.J. 2/25/14 @ p. 5.
- *Note, "Understanding and Authenticating Evidence From Social Networking Sites,"* 7 Wash. J.L. Tech. & Arts 209 (2012)

The End

Thanks to Jim Fagan for Assistance in the Preparation of this Presentation

10/916