NYSBA FAMILY LAW SECTION
ANNUAL SUMMER MEETING

JULY 12, 2019

TECHNOLOGY, SOCIAL MEDIA AND ETHICS IN THE COURTROOM

Stephen Gassman, Esq.
Gassman Baiamonte Gruner, PC
Garden City, N.Y. 11530

Pamela M. Sloan, Esq.
Aronson, Mayefsky & Sloan LLP
New York, N.Y.

Contents

ISSUES WITH SOCIAL MEDIA

I. UBIQUITOUS NATURE OF SOCIAL MEDIA

A. Statistics

1. Facebook has approximately 1.8 billion users worldwide, 214 million in USA.

2. 250 billion photos are uploaded to Facebook every day

3. LinkedIn has some 500 million total users.

4. Twitter, created in March 2006, has 321 million active monthly users, with over 500 million tweets made per day as of late 2018.

5. 2018 Pew Research Center Study of social media reports that 69% of the general public uses some kind of social media.

B. Our daily inadvertent exposure to social media and technology

1. GPS tracker and electronic control modules ("black boxes") in motor vehicles

a. When you leave your house, probably the neighbors exterior camera catches you on film. When you are driving your car, if you have a navigation system, signals are sent to a satellite and stored in the cloud. The information is sold to leasing companies, etc., and can also be deemed a business record.

b. rental car companies, fleet trucking companies

2. Home video doorbells and wireless security devices

C. Hacking

D. Use of Social Media in Litigation

1. It is likely that the modern witness has an electronic trail.

2. Issue of who will testify when you get information on social media in your office

3. Google Glass has been used to create day-in-the-life videos of injured individuals.

II. ATTORNEYS' RESPONSIBILITY

A. Rule 1.1 of the ABA's Model Rules, dealing with the duty of competence.

1. Comment 8: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the *benefits and risks associated with relevant technology,*…"

B. Consistent with Comment 8 – NY Rules of Professional Conduct (RPC) 1.1 states:

1. A New York lawyer should: "keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information".

C. Confidentiality Issue - RPC 1.6

1. As part of preserving client confidences, lawyers need to take reasonable care to ensure that only authorized individuals have access to electronic files.

2. "When transmitting any communication that relates to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty does not require that the lawyer used special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of a lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the information is protected by law or a confidentiality agreement."

3. Responding to Negative Online Review

a. Does not trigger the exception to NY Rules of Professional Conduct 1.6 (Confidentiality of Information) that in other circumstances permits a lawyer to reveal confidential information to establish a defense to a controversy between the lawyer and client, or to respond the allegations relative to the lawyer's representation of the client.

D. ABA Formal Opinion 483 (2018) – Lawyer's Obligations after a Data Breach or Cyberattack

1. Before a breach occurs, it is recommended that lawyers design an "incident response plan" designed to identify and stop a breach, mitigate

any loss or theft of data, restore system security and eventually restore the firm's system itself.

2. It is not a violation of Rule 1.6 of Model Rules (dealing with preserving client confidences) if data is lost or accessed if the lawyer made reasonable efforts to prevent the loss or access.

3. There is a duty to inform a current client of a data breach that impacts their material confidential information.

E. Areas of technological competence:

1. Data security
2. Practice management technology
3. Social media competence
4. Technology used by clients to build products or offer services that lawyers have to defend
5. Electronic discovery
6. Technology used to present information in court[1]

F. Court Rules

1. Rules 202.12 (b) and 202.70 (g) of New York's uniform trial court rules requires all attorneys be sufficiently versed in matters relating to their clients technological systems to be competent to discuss all issues relating to electronic discovery at preliminary conferences.[2]

2. if a lawyer lacks the requisite skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate with another attorney or expert who possess the skills. RPC 1.1 (b).

III. TALES OF WOE – AVOIDING TROUBLE

A. Judges

1. A Wisconsin appellate court held that a judge's undisclosed

---

[1] / See Davis and Pulszis, "An Update on Lawyers' Duty of Technological Competence: Part 1", NYLJ, 3/1/19; Part 2, NYLJ, 5/3/19

[2] / Notice amending Section 202.12(b) of the Uniform Rules as well as Rule 1(b) of section 202.70(g) and requiring that in any case "reasonably likely to include electronic discovery" counsel must come to court "sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery" and may bring a client representative or outside expert to assist in such discussion.

22 NYCRR 202.12(c)(3)(i) – At a preliminary conference, a matter to be considered is "retention of electronic data and implementation of a data preservation plan".

Facebook "friendship" with a litigant amounted to objective bias and violated due process. *In re: The Paternity of B.J.M.; Miller v. Carroll (Wis. App. Ct., Feb. 2018)*

2. The Florida Supreme Court, in *Law Offices of Herssein & Herssein, P.a. v. United Servs. Auto. Ass'n*., 2018 WL 5994243 (Fla. Sup. Ct., 11/15/18), in a 4 – 3 decision, held that a judge's mere Facebook "friendship" with a lawyer involved in the case before him was not a basis for disqualification. In doing so, the judge has rejected a Florida judicial ethics advisory committee advice that judges should not "friend" lawyers who appear before them.

3. A Colorado Appeals Court judge was forced to resign after her former lover disclosed her emails with demeaning references about her colleagues. She referred to a fellow appeals judge, a Latina, as "the little Mexican." She referred to her ex-boyfriend's wife, who is Native American, as "the squaw."

4. A New Mexico judge was forced to resign because of the sexual nature of the text messages he sent to his wife, a court employee in the same courthouse, while he was conducting a jury trial.

B. Lawyers

1. In what is being called the largest E discovery sanction penalty ever leveled directly against an attorney, a Virginia state judge ordered lawyer Matthew Murray to pay $542,000 for instructing his client to remove photos from his Facebook profile, and for his client to pay an additional $180,000 for following the instructions. *Lester v. Allied Concrete Co.*, 2011 Va. Cir. LEXIS 245 (Va. Cir. Ct. 2011 Sept. 6, 2011)
The wrongful death plaintiff lost his young wife in a tragic accident,

IV. LITIGATION HOLDS FOR ESI; SPOILATION

A. Duty to Preserve Evidence

1. Voom HD Holdings, LLC v. Echostar Satellite, LLC, 93 AD3d 22, 939 NYS2d 321 (1st Dept. 2012)

a. Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents, which hold is not limited simply to avoiding affirmative acts of destruction; since

computer systems generally have automatic deletion features that periodically purge electronic documents such as e-mail, the party facing litigation must take active steps to halt that process.

b. The hold must direct appropriate employees to preserve all relevant records, electronic or otherwise, and create a mechanism for collecting preserved records so that they might be searched by someone other than the employee.

c. The hold should, with as much specificity as possible, describe the electronically stored information at issue, direct that routine destruction policies such as auto-delete functions and rewriting over e-mails cease, and describe the consequences for failure to so preserve electronically stored evidence.

2. Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212 (SDNY 2013)- "once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of routine documents."

3. The duty to preserve is extended to electronically stored information, including email and other electronic documents. *(915 Broadway Associates LLC v. Paul, Hastings, Janofsky & Walker*, 34 M3d 1229(A), 950 NYS2d 724 (S.Ct., N.Y. Co., 2012, Fried, J.)

B. Spoliation

1. Spoliation is the destruction or significant alteration of evidence or the failure to preserve property for another's use as evidence in pending litigation or even before litigation is commenced where that litigation is reasonably foreseeable. *Voom HED Holdings v. EchoStar Satellite LLC, supra.*

C. Sanctions for Spoliation

1. *Pegasus Aviation I, Inc. v. Varig Logistica, S.A.*, 26 NY3d 543, 26 NYS3d 218 (2015) – A party that seeks sanctions for spoliation of evidence must show that:

a. the party having control over the evidence possessed an obligation to preserve it at the time of its destruction,

b. that the evidence was destroyed with a "culpable state of mind" and

c. the destroyed evidence was relevant to the party's claim or defense such that the trier of fact could find that the evidence would support that claim or defense.

2. Relevancy

a. Where the evidence is determined to have been intentionally or willfully destroyed, the relevancy of the destroyed documents is presumed.

b. On the other hand, if the evidence is determined to have been negligently destroyed, the party who seeks spoliation sanctions must establish that the destroyed documents were relevant to the party's claim or defense.

c. An adverse inference charge may be appropriate even where the evidence was found to have been negligently destroyed.

3. Striking of Pleadings

a. Defendant's pleadings properly struck where defendant destroyed emails relevant to plaintiff's defamation action. Where a party disposes of evidence without moving for a protective order, a negative inference may be drawn that the destruction was willful. Willfulness may also be inferred from a party's repeated failure to comply with discovery directives. *Chan v. Cheung*, 138 AD3d 484, 30 NYS3d 613 (1st Dept. 2016)

4. Adverse Inference

a. Where the spoliation is the result of plaintiff's intentional destruction or gross negligence, the relevance of the evidence lost or destroyed is presumed. Generally, dismissal of a complaint is warranted only where the spoliated evidence constitutes the sole means by which the defendant can establish its defense or where the defendant was otherwise "fatally compromised" or rendered "prejudicially bereft of its ability to defend as a result of the spoliation. Here, given the massive document production and the key witnesses that are available to testify, an adverse inference charge is an appropriate sanction. *Arbor Realty Funding v. Herrick, Feinstein,* 140 AD3d 607, 36 NYS3d 2 (1st Dept. 2016)

D. Smartphone

1. *Leah F. v. Ephraim F.*, 56 Misc3d 1210(A), 63 NYS3d 305 (Family Co., Kings Co., Vargas, J.)(2017 WL 3185118)(Jul. 24, 2017) – Where wife took possession of Husband's smartphone and "copied" it in violation of a court order, the Husband's motion to hold wife in contempt denied upon finding that no prejudice was created that would infringe on rights of either party notwithstanding a finding that the wife violated a clear and lawful mandate of court. In Family Court proceeding, a finding of civil contempt may be established by the well-settled clear and convincing evidence standard. To sustain finding of civil contempt, the court must find that the alleged contemnor violated a lawful order of the court, clearly expressing an unequivocal mandate, of which the party had knowledge, and that as a result of violation a right of a party to litigation was prejudiced.

Nevertheless, wife/her agents precluded from using any copy of the contents of husband's smartphone in this or any other proceeding in Family Court, and that any data or copies of phone retained by wife and her counsel should be returned to husband and his counsel as husband had reasonable expectation of privacy in phone and any evidence obtained through device without his permission should be excluded. affd., *Fruchthandler v. Fruchthandler*, 161 AD3d 1151, 78 NYS3d 214 (2d Dept. 2018)

E. Spyware

1.Where husband installed spyware on the wife's iPhone and then used that spyware to monitor his wife's communications, including more than 200 privileged emails with her attorney, and then purposefully engaged in spoliation of the evidence while simultaneously asserting his Fifth Amendment right against self-incrimination, the Court struck his pleadings seeking spousal support, equitable distribution and counsel fees. *Crocker C. v. Anne R.*, 58 M3d 1221(A) (Supreme Court, Kings Co., 2018, Sunshine, J.)

V. FACEBOOK POSTS AND PRODUCTION OF FACEBOOK POSTINGS – The Game Changer - *Forman v. Henkin*, 30 NY3d 656, 70 NYS3d 157 (2018)

A. Prior to Forman

1. Factual predicate required – Forman effectively overrules *Tapp v. NYS Urban Dev*., 102 AD3d 620 (1st Dept. 2013) which required defendant seeking disclosure from a plaintiff's Facebook account to establish a factual predicate by identifying information in the account that "contradicts or conflicts with the plaintiff's alleged restrictions, disabilities, and losses, and other claims."

B. Five Takeaways from Forman

1. Material and Necessary Standard

a. There is nothing so novel about Facebook materials that precludes the application of NY's long-standing disclosure rules to resolve disputes, i.e., the "material and necessary" standard enunciated by CPLR 3101(a).

b. In a contested custody action, the husband sought an order directing wife to turn over printouts of all pictures, posts and information posted on her Facebook pages over 4 years, claiming such disclosure would be relevant and material to the issue of the amount of time the wife had

spent with the child since birth. The court held that the time spent by the parties with the child may be relevant and material and thus ordered defendant to produce for an in camera review printouts of her Facebook postings depicting or describing her whereabouts, outside the New York City area, from the time of child's birth to the commencement of the proceeding, and to provide an affidavit describing the printouts in general terms and also requiring defendant to provide an authorization permitting the court to have access to her Facebook postings during the applicable time period. The court also *sua sponte* directed plaintiff, the moving party, to produce all of defendant's postings that he possessed or had access to with an affidavit stating that they represent all such Facebook postings possessed by or available to defendant in their entirety during such time. *A.D. v. C.A.*, 50 M3d 180, 16 NYS3d 126 (Sup. Ct., Westchester Co., 2015, Ecker, J.)

c. In awarding the father custody, the court took into account as part of the mother's inappropriate behavior, her utilization of Facebook to insult and demean the child, who was then 10 years old, by, among other things, calling him and "ass hole." She testified without remorse that she did so because that is what "[h]e is," and she thought it was important for her Facebook friends to know this. [Court: "Charitably stated, her testimony reflected a lack of insight as to the nature of her conduct toward her oldest child."] *Melody M. v. Robert M.,* 103 AD3d 932, 962 NYS2d 364 (3d Dept. 2013)

d. Audit Trail of Electronic Records

(1) Vargas v. Lee, 170 AD3d 1073, 96 NYS3d 567 (2d Dept. 2019) - Plaintiff moved to compel the hospital to produce the audit trail of the plaintiff's electronic medical records from May 1, 2012 (the date of the surgery) until May 17, 2012. In the trail is the metadata that essentially indicates what changes are made to electronic record each time it was accessed. Citing *Forman*, the Appellate Division held that the portion of the audit trail at issue was reasonably likely to yield relevant evidence bearing directly upon the postoperative care. Moreover, the request was limited to the period immediately following the surgery and the disclosure would also assist preparation for trial by enabling counsel to ascertain whether the patient records that were eventually provided to them were complete and unaltered.

e. Material and Necessary Requirement – Not Met

(1) Fawcett v. Altieri, 38 M3d 1022, 960 NYS2d 592 (S.Ct., Richmond Co., 2013) – A court is required to determine whether the content contained on the social media account is material and necessary, and then to balance whether the production of the contents would result in a violation of the account holder's privacy rights.

(2) Subpoenas at issue must be quashed. Not only has the husband failed to establish that the telephonic and internet information sought about the Wife is relevant and material to this action, but no special circumstances permitting a non-party disclosure has been shown. The Husband claims that the Wife's telephone logs and AOL instant messages chat logs would be relevant to the issue of custody and equitable distribution. While the Wife's fitness for custody is certainly in issue herein, this Court is not persuaded that any purpose would be served by permitting disclosure of these telephonic and AOL logs. Indeed, these logs or lists will only show that the Wife was on the phone or online with friends and relatives during certain periods of time; they would not reveal the nature of the conversations or her state of mind. The Court does not believe these telephone and computer records are necessary for a custody determination. *Bill S. v. Marilyn S.*, 8 Misc3d 1013(A), 801 NYS2d 776 (S.Ct., Nassau Co., 2005, Balkin, J.)

2. Rejects Factual Predicate Standard

a. Rejects notion that there is a heightened standard for the production of social media requiring a party to establish "a factual predicate" for their request by *identifying relevant information in the opposing party's* Facebook account.

3. Items Need not Exist

a. Disclosure is not conditioned upon a showing that the items sought actually exist; rather, the request need only be appropriately tailored and reasonably calculated to yield relevant information.

4. "Privacy" Setting

a. An account holder's so-called "privacy settings do not govern the scope of disclosure on social media materials." Even private materials may be subject to discovery if they are relevant.

b. *Romano v. Steelcase, Inc.*, 30 Misc3d 426, 907 NYS2d 650 (S.Ct., Suffolk Co., Spinner, J. – A plaintiff must give the defendant access to her private postings from two social network sites, Facebook and MySpace, that could contradict claims she has made in a personal injury action. The Court commented that:

> "As the public portions of plaintiff's social networking sites contained material contrary to her claims in deposition testimony, there is a reasonable likelihood that the private portions of sites may contain further such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the offense of this action…."[W]hen plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of the social networking sites or else they would cease to exist…[I]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking."

5. Remedy to Account Holder

a. To the extent an account may contain sensitive or embarrassing materials of marginal relevance, the account holder can seek protection from the court.

b. Balancing test as to whether the production of the content would result in a violation of the account holder's privacy rights. (see, *Peo. v. Harris*, 36 M2d 613, 945 NYS2d 505 (Crim. Ct., NY Co., 2012); *Peo. v. Harris*, 36 M2d 868, 949 NYS2d 590 (Crim. Ct., NY Co., 2012) (Subpoena issued to online social networking service provider, seeking user postings and account information, was proper under the Stored Communications Act (SCA), so long as the material sought was relevant and evidentiary; user had no reasonable expectation of privacy in his postings, since they were made public, and provider would not be unduly burdened by the request. 18 U.S.C.A. § 2703(d).)

VI. POST *FORMAN v. HENKIN*

A. Injunctive Relief

1. Defendants have shown the necessity for a temporary order and

preliminary injunction restraining Plaintiff from directly, or indirectly through other persons, modifying, changing or deleting any information from his social networking accounts relating to this action. Plaintiff originally denied possessing any social media accounts during his deposition. However, medical records relating to Plaintiff's hospitalization related to an alleged suicide attempt and revealed Plaintiff made suicidal statements on his Facebook account. Plaintiff then deleted/deactivated his Facebook account on the alleged advise from his legal counsel to aid him in this action. With Plaintiff's inclination to delete/deactivate his Facebook account (and potentially other social media accounts), Plaintiff must be temporarily retrained from modifying, changing or deleting any statements related to this action made on his social media accounts for the duration of this action. *Paul v. the Witkoff Group* 2018 WL 1697285 (N.Y. Sup. Ct. Apr. 03, 2018, Mendez, J.)

B. Overbroad Demand

1. The Appellate Division rejected a demand for access to social media accounts for 5 years prior to the incident and to cell phone records for 2 years prior to the incident as "overbroad and not reasonably tailored to obtain discovery relevant to the issues in the case and instead approved production for a period of 2 months before the date on which plaintiffs were allegedly attacked on defendant's premises to the present. *Doe v. Bronx Preparatory Charter School,* 160 AD3d 591, 76 NYS3d 126 (1st Dept. 2018)

C. Can precede deposition

1. Nothing in *Forman v Henkin* indicates that a party must wait until after a deposition before demanding disclosure of the private portions of an individual's social media account. Indeed, such a rule has the potential to needlessly delay disclosure of relevant information. *Christian v. 846 6th Ave. Property Owner, LLC*, 2018 WL 2282883 (Supreme Court, NY Co., Freed, J.)

D. Access to plaintiff's accounts and devices

1. In personal injury action, plaintiff's private social media information was discoverable, albeit with some limitations on the time span and subject matter. Access was given to third party data mining company to uncover items on plaintiffs private social media accounts and devices. *Vasquez-Santos v. Mathew*, 168 AD3d 587, 92 NYS3d 243 (1st Dept. 2019)

VII. OTHER SOCIAL MEDIA DISCOVERY

A. E-Mails Directly

1. Defendant was directed to produce hard copies of all e-mail messages relating to designated allegations, including any e-mail messages that have been deleted but may be recovered by a qualified expert appointed by referee supervising disclosure for an in camera inspection and a determination of which documents in fact deal with the designated allegations and only those e-mails will be turned over to plaintiff. *Samide v. Roman Catholic Diocese of Brooklyn,* 5 AD3d 463, 773 NYS 116 (2d Dept. 2004)

2. Authorization to obtain ESI

a. In a family offense proceeding, alleging that respondent sent petitioner numerous vulgar e-mails, respondent was directed to execute authorizations for Yahoo, respondent's Internet e-mail service provider, and to produce e-mails from respondent to petitioner during a given period of time. While the CPLR does not expressly provide for authorizations to obtain Internet, computer or e-mail records, the purpose of pretrial disclosure is to permit parties to discover material and necessary evidence for use at trial. *D.M. v. J.E.M.*, 23 M3d 584, 873 NYS2d 447 (F.Ct., Orange Co., 2009, Kiedaisch, J)

b. Court required plaintiff to deliver "a properly executed consent and authorization" to obtain Facebook and MySpace information. *Romano v. Steelcase, Inc*., 30 Misc3d 426, 907 NYS2d 650 (S.Ct., Suffolk Co., Spinner, J.

B. Effect of Discovery

a. Where plaintiff, and a deposition, was confronted with 13 pages of printouts allegedly from his Facebook account and denied that they were from his accountant, and then sought to depose the individual who obtained the printouts, defendant would be precluded from offering the printouts at trial unless he produce such person for a deposition, as plaintiff would be left with no other means to prove or disprove the authenticity*. Lantigua v. Goldstein*, 149 AD3d 1057, 53 NYS3d 163 (2d Dept. 2017)

C. *cf.* Grounds for Divorce - *Bill S. v. Marilyn S.*, 8 M3d 1013, 801 NYS2d 776 (S.Ct., Nassau Co., Balkin J.) – Court quashed subpoenas duces tecum served by the husband for telephone and chat logs relating to alleged paramours of the wife. Husband was not entitled to pretrial discovery with respect to the issue of grounds for the divorce or marital fault. He failed to establish how the records sought are relevant and material, and failed to show special circumstances permitting non-party disclosure.

VIII. COMPUTERIZED BILLING RECORDS

A. At the trial of an action for unpaid legal fees, plaintiff's managing partner testified that plaintiff's electronic billing records – which identified the attorney or paralegal who rendered services to defendants, the tasks performed, and the time spent on each task – were created contemporaneously with the services performed, in the normal course of plaintiff's business. The Court held that the testimony of the managing partner was sufficient to lay the foundation for the admission of the records under the business record rule, "without the necessity of calling multiple witnesses who would have merely offered cumulative testimony at best". *Finkelstein Newman Ferrara LLP v. Avemm Corp*. 36 Misc3d 144(A), 2012 NY Slip Op 51587 (App. Term, 2012)

IX. JUDICIAL NOTICE; WEB MAPPING SERVICE

A. CPLR Rule 4511(c): When judicial notice shall be taken based on a rebuttable presumption.

> Every court shall take judicial notice of an image, map, location, distance, calculation, or other information taken from a web mapping service, a global satellite imaging site, or an internet mapping tool, when requested by a party to the action, subject to a rebuttable presumption that such image, map, location, distance, calculation, or other information fairly and accurately depicts the evidence presented. The presumption established by this subdivision shall be rebutted by credible and reliable evidence that the image, map, location, distance, calculation, or other information taken from a web mapping service, a global satellite imaging site, or an internet mapping tool does not fairly and accurately portray that which it is being offered to prove. A party intending to offer such image or information at a trial or hearing shall, at least thirty days before the trial or hearing, give notice of such intent, providing a copy or specifying the internet address at which such image or information may be inspected. No later than ten days before the trial or hearing, a party upon whom such notice is served may object to the request for judicial notice of such image or information, stating the grounds for the objection. Unless objection is made pursuant to this subdivision, or is made at trial based upon evidence which could not have been discovered by the exercise of due diligence prior to the time for objection otherwise required by this subdivision, the court shall take judicial notice of such image or information.

X. PROHIBITIONS FROM POSTING

A. The family court prohibited the mother from posting on Facebook, Twitter or any other social media site any mention of the child, the father or any members of their household. The mother had a history of disparaging the father and his new family on Facebook, but did not mention the parties own child. The appellate court reversed the prohibition against her posting communications about the child who she had never previously disparaged. *Matter of Driscoll v. Ourster*, 146 AD3d 1179 (3d Dept. 2017)

B. Following a hearing, which lasted over 55 days, the court granted the father's motion for suspension of the mother's parental access to her daughter of any kind and in any form, including telephone, Skype, email, and social media. *S.B.S. v. S.S.,* NYLJ, 4/3/18, Supreme Court, Nassau Co., Bennett, J.

XI. ISSUE OF EXPECTATION OF PRIVACY

A. E-Docs Stored at Work

1. Physician's e-mail communications with his attorney, which e-mails were stored on defendant-hospital's e-mail server, were not confidential, for purposes of attorney-client privilege, where hospital's electronic communications policy, of which the physician had actual and constructive notice, prohibited personal use of hospital's e-mail system and stated that hospital reserved the right to monitor, access, and disclose communications transmitted on hospitals e-mail server at any time without prior notice, though physician's employment contract required hospital to provide him with computer equipment. *Scott v. Beth Israel Med. Ctr*., 17 Misc3d 934, 847 NYS2d 436 (S.Ct., N.Y Co. 2007, Ramos, J.)

2. An employee used a work-issued laptop to e-mail confidential files to her attorney purportedly in contravention of her employers "work only" use policy. As the employee used the work computer to send the e-mails from home through her personal AOL account (and thus, the documents never "assed through" the employer's system), the court found that the privilege was not waived. *Curto v. Medical World Communications Inc.*, 2006 WL 1318387 (EDNY, 5/16/06)

3.In determining whether there has been a waiver of the attorney-client privilege when an office computer is used to communicate with attorney, the court evaluates: (1) whether the employer's policies permit or prohibit personal use; (2) whether the company monitors use of the employee's email; (3) whether third parties have a right of access; and (4) whether the company advised the employee or whether the employee was aware of the use and monitoring policies. *U.S. v. Finazzo*, 543 F. Supp 2d 224, 2008 U.S. Dist. LEXIS 30604 (SDNY Mar. 26, 2008)

B. Cell Phone Tracking

1. Cell Phone Tracking - technique whereby phone calls allegedly made from one's cell phone may be used to determine the approximate location of the cell phone use when making the calls.

2. CSD - cell phone data

3. A cell phone user has no "reasonable" expectation of privacy that the devices built in global positioning technology will not be used by police to locate the phone. Through a person's voluntary utilization of the cell phone, which occurs when the device is powered up, "a person necessarily has no reasonable expectation of privacy with respect to the phone's location." While cell phone users could maintain a reasonable expectation of privacy about the *content* of the conversations, the same does not apply to the process of physically locating the devices. Accordingly, after finding the defendant's cell phone number, the police filled out an "exigency circumstances request" asking for Sprint to "ping" or locate the phone. *People v. Moorer*, 39 Misc3d 603, 959 NYS2d 868 (County Ct., Monroe Co., 2013, DeMarco, J.)

4. The Stored Communications Act, which prohibits accessing without authorization a facility through which electronic communication services provided and thereby obtaining access to electronic communication while it is in electronic storage, does not apply to data stored in a personal cell phone. A personal cell phone is not a "facility" as contemplated by the statute and the information is not in "electronic storage". *Garcia v. City of Laredo*, No. 11-41118 (U.S.C.A., 5th Cir., 2012)

5. A driver who hit a pedestrian can introduce the pedestrians cell phone records into evidence in order to argue that the pedestrian contributed to the accident by talking on the phone. *Miller v. Lewis*, NYLJ, 4/25/13 (S.Ct., Kings Co., Ruchelsman, J.)

C. GPS Devices

1. Civil Case - *Matter of Cunningham v. NYS Department of Labori*, 21 NY3d 515, 974 NYS2d 896 (2013) – Government can attach a GPS tracking device to a public employee's personal vehicle without a warrant. When an employee chooses to use his car during the business day, GPS tracking of the car may be considered a workplace search, and public employees have a diminished right of privacy in the workplace if a search satisfies a standard of reasonableness (*O'Connor v. Ortega*, 480 US 709 [1987])

2. Criminal Case - *People v. Weaver,* 12 NY3d 422 (2009) - the state Constitution bars the government from placing a GPS device on a criminal suspects vehicle without a warrant; *United States v. Jones,* 132 S.Ct. 945 (2012) – the Fourth amendment bars the warrantless installation of a GPS device on a criminal suspects vehicle.

D. Email Signatures

1. Although a typed name on an email is the equivalent of a signature, the same is not true for an attachment to an email, which can easily be signed by the sender. Thus, plaintiff's breach of contract theory depended upon an attachment to an email sent by the defendant to plaintiff. Because the attachment was not signed, there was no contract. *Solartech Renewables, LLC v. Vitti*, 156 AD3d 995, 66 NYS3d 704 (3d Dept. 2017)

2. An email message may be considered "subscribed" as required by CPLR 2104, and, therefore, capable of enforcement, where it "contains all material terms of a settlement and a manifestation of mutual accord, and the party to be charged, or his or her agent, types his or her name under circumstances manifesting an intent that the name be treated as a signature" (*Forcelli v. Gelco Corp.,* 109 AD3d at 251, 972 NYS2d 570). Here, the email confirming the settlement agreement was sent by counsel for the party seeking to enforce the agreement, LICO. There is no email subscribed by the plaintiff, who is the party to be charged, or by her former attorney. In the absence of a writing subscribed by the plaintiff or her attorney, the settlement agreement is unenforceable against the plaintiff (*see id.* at 248, 972 NYS2d 570; *see also* CPLR 2104). *Kataldo v. Atl. Chevrolet Cadillac*, 2018 N.Y. Slip Op. 03669 (2d Dept. 2018)

E. Family Court did not err in admitting messages obtained by father on mother's Facebook account where the account was available on son's Ipod without password protection. *Rutland v. O'Brien*, 143 AD3d 1060, 41 NYS3d 292 (3d Dept. 2016)

XII. INADVERTENT DISCLOSURE OF PRIVILEGED E-MAIL

A. Statute – CPLR 4548. "No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.

B. Inadvertent disclosure of a document protected by the attorney-client privilege, will not constitute a waiver of the privilege. An intent to waive the privilege by disclosure of the document must be shown, in order to have a valid waiver. *Manufacturers and Traders Trust Co. v. Servotronics, Inc.,* 132 AD2d 392, 398, 522 NYS2d 999 (4th Dept. 1987).

C. Defendant's counsel, in motion papers, inadvertently had attached as

an exhibit pages of documents that were protected by the attorney-client privilege. **"**Here, it is clear that the disclosure was inadvertent and unintentional. Upon finding that the e-mail had been turned over to plaintiffs' counsel, Grossman immediately took steps to demand its return." *Galison v. Greenberg*, 5 Misc.3d 1025(A) (S.Ct., NY Co., 2004, Cahn, J.)

D. Ethics Opinion

1. N.Y. Rules of Professional Conduct Rule 4.4(b) – "[a] lawyer who receives a document, electronically stored information, or other writing relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

2. Cautionary Note to Rule 4.4, Comment 2: "a lawyer who reads or continues to read a document that contains privileged or confidential information may be subject to court-imposed sanctions, including disqualification and evidence-preclusion."

E. Waiver of Privilege

1. *AFA Protective Systems, Inc. v. City of New York*, 13 AD3d 564, 788 NYS2d 128 (2d Dept. 2004): "disclosure of a privileged document results in waiver of the privilege unless the party asserting the privilege meets its burden in proving that (1) it intended to maintain confidentiality and took reasonable steps to prevent its disclosure, (2) it promptly sought to remedy the situation after learning of the disclosure, and (3) the party in possession of the materials will not suffer undue prejudice if a protective order is granted. Here, defendant waived the privilege by failing to exercise due diligence where defendant knew for approximately 4 years that the memo in question was in the possession of third parties who could make copies of it, use it and disseminate information contained therein and defendant took no action to retrieve the document for four years. (See also, *John Blair Communications, Inc. v. Reliance Capital Group, L.P.*, 182 AD2d 578, 582 NYS2d 720 [1st Dept. 1992])

2. While an inadvertent production of a privileged work product document generally does not waive the applicable privilege, there is an exception to that rule if the producing party's conduct "was so careless as to suggest that it was not concerned with the protection of the asserted privilege" (*Securities & Exch. Commn. v Cassano*, 189 FRD 83, 85 [SD NY 1999]; *Scott v Beth Israel Med. Ctr. Inc.*, 17 Misc 3d 934, 943, 847 NYS2d 436 [Sup Ct 2007]

F. Improperly Obtained Discovery

1. Recusal - In a trust accounting proceeding, a law firm which covertly issued subpoenas and employed deceitful and unprincipled means to secure discovery of confidential and privileged material from the adverse party's former law firm without notifying that party, must be disqualified from further participation in the proceeding since there is no other way of assuring that the tainted knowledge improperly obtained will not subtly influence the firm's conduct of the litigation. *Matter of Beiny*, 129 AD2d 126, 517 NYS2d 474 (1st Dept. 1987)

2. If, during pre-trial disclosure, confidential communications between an adversary and counsel are improperly obtained, the information thus acquired may be suppressed pursuant to CPLR 3103 (see), and the lawyer who, or law firm which, obtained the information may be disqualified from continuing as counsel in the action.

3. Dismissal of Action - Plaintiff's complaint dismissed as a remedy for her misconduct that involved the taking and use of her adversary's privileged documents. *Lipin v Bender*, 84 NY2d 562, 620 NYS2d 744 [1994]

XIII. USE OF POWER POINT PRESENTATIONS AT TRIAL

A. *People v. Williams*, 29 NY3d 84, 52 NYS3d 286 (2017)

1. There is no inherent problem with the use of a PowerPoint presentation as a visual aid in connection with closing arguments.

2. The PowerPoint materials must be limited to characterizations of facts that are “within the four corners of the evidence” and not allow jurors to draw conclusions which are not fairly inferable from the evidence.

3. If counsel is going to superimpose commentary to images of tri al exhibits, the annotations must accurately represent the trial evidence.

B. *People v. Anderson*, 29 NY3d 69, 52 NYS3d 256 (2017)

1. PowerPoint slides depicting an already admitted photograph with captions accurately tracking prior testimony might reasonably be argued as relevant and fair commentary on the evidence.

XIV. EMAIL AS BASIS FOR ORDER OF PROTECTION

A. For the Court to issue an order of protection, there must be a family offense as described in FCA §812, DRL §252. The selected statutes follow the Penal Law wording, except to the extent that "disorderly conduct" (PL §240.20) includes disorderly conduct not in a public place. Plaintiff asserts defendant's emails constitute a form of harassment. To the extent defendant admits authorship and sending the emails, the order of protection could be issued without a hearing. Defendant concedes that emails can be the basis of a family offense. *L.T. v. K.T.*, 47 M3d 1211(A), 15 NYS3d 712 (S.Ct., Putnam Co., 2015, Grossman, J.)

B. In connection with Aggravated Harassment in the Second Degree, and email falls within a "mechanical or electronic means". The email in question which formed the basis of a finding that with intent to threaten or alarm the petitioner, respondent initiated a mechanical or electronic communication in written form in a manner that did, in fact, cause annoyance or alarm, stated as follows: "You stand accused of having a sexual predatory relationship with my son [name deleted]. You also picked up the body at a [name deleted] morgue last summer. It was used. You received a fat check for your activities. I am putting you on notice*." M.G. v. C.G.*, 19 M3d 1125, 862 NYS2d 815 (Singer, J.)

C. Evidence established that father committed family offense of harassment in the second degree, where mother testified that 294 e-mails which father sent her during approximately eight-month period made her feel disgusted and physically ill, and that she repeatedly asked him to stop sending her e-mails not directly related to visitation. Father acknowledged sending e-mails, and text of e-mail messages showed that most served no legitimate purpose, but were harassing, annoying, insulting, or abusive. *Julie G. v. Yu-Jen G.*, 81 AD3d 1079, 917 NYS2d 355, (3d Dept. 2011)

D. Violations of Order of Protection

1. Where TOP directed father to refrain from communication or any other conduct by mail, telephone, voicemail or other electronic or any other means with the mother, and not to call her at work, but may contact the mother, other than at work, in the event of an emergency regarding the child for visitation arrangements, father's email to mother regarding custody dispute over child were not sent with the intention of harassing, annoying or alarming mother, and his one phone call to mother's work because she had been unresponsive to his efforts to facilitate custody order was made for a legitimate purpose. However, father's email accusing mother of child abuse and sending her a communication that did not relate to an emergency

regarding the child for visitation arrangements was a violation of the TOP. *Lisa T. v. K.T.*, 49 M3d 847 14 NYS3d 883 (Fam. Ct., Bronx Co., 2015, Kelley, J.)

2. The order of protection prohibited defendant from contacting the victim by "electronic or any other means." Defendant was charged with criminal contempt in the second degree upon the ground that she allegedly "tag" the protected party in two Facebook posts, stating ""Stupid" and "You and your family are sad…" , You guys have to come stronger than that!! I'm way over you guys but I guess not in ya agenda." The victim alleged in her supporting deposition that she had received a Facebook notification stating that the defendant attacked her in the above post. Defendant's motion to dismiss the accusatory instrument as facially insufficient was denied, the court finding the allegations to be "sufficient for pleading purposes to establish a violation of the order protection. *People v. Gonzalez*, N.Y.L.J., 1/15/16 (S.Ct., Westchester Co., Capeci, A.J.)

3. Indirect Transmission - While the record supports Family Court's determination that the father willfully violated the February 2009 temporary order of protection, a violation of the July 2009 order is not sufficiently established. The February 2009 order prohibited, as relevant here, the father from communicating with the mother by e-mail and ordered that he "avoid all contact, direct or indirect" with her. The mother's sister—who stated that she had a "very close" relationship with the mother and had not communicated with the father in a "very long time"—received an e-mail from the father shortly after the order of protection was issued. The e-mail, which ostensibly was initially directed to the sister's husband, contained scurrilous accusations about the mother and her family. The sister promptly forwarded the e-mail to the mother. Under the circumstances, the evidence was sufficient to support the Family Court's conclusion that the father knew or intended that, by sending the e-mail to the mother's family, it would reach the mother (*see Matter of Duane H. v. Tina J.,* 66 AD3d 1148, 1149, 887 NYS2d 345 [2009]). *Jennifer G. v. Benjamin H.,* 84 AD3d 1433, 1435, 923 NYS2d 249, 252-53 (3d Dept. 2011)

4. Violation petition of a "refrain from" order of protection not sustained, upon motion to dismiss, by allegations that respondent called and emailed petitioner, and sent her text messages demanding that she let him move back into the party's house and demanding his belongings. The petitioner failed to adequately allege that the respondent, acting with the requisite intent that is inferable from the alleged circumstances, engaged in the offense of aggregated harassment in the second degree or harassment in the second degree. *Cote v. Berger*, 112 AD3d 821, 978 NYS2d 54 (2d Dept. 2013)

XV. ACCESS TO HOME OR SPOUSE'S COMPUTER

A. Access Granted

1. Information stored by husband on laptop computer, albeit password protected, subject to disclosure in matrimonial action where wife sought access on grounds that husband stored information thereon concerning his finances and personal business records. As the laptop was in the marital residence, it was akin to a filing cabinet to which the wife clearly would have had access. *Byrne v. Byrne*, 168 M3d 321, 650 NYS2d 499 (S.Ct., Kings Co., 1996, Rigler, J.)

2. Information stored on the husband's computer was not subject to suppression, and wife's access to the information was not without authorization as the husband had consented to the wife's access to his computer. *White v. White*, 781 A.2d 85 (N.J. Super. Ct. 2001)

3. Husband moved to suppress data obtained by wife from the hard drive of a computer she found in the trunk of husband's car, the Wife claiming it was a shared family computer and the husband claiming it was his personal computer issued to him by his employer. The Court refused to grant the suppression motion. *Moore v.* Moore, NYLJ, 8/14/08, p.26 col.1 (S.Ct., NY Co., Evans, J.) –

4. In a matrimonial action, the wife was entitled to have her computer expert copy data from the hard drives of husband's personal and business computers, and to examine hard copies of non-privileged business records identified by referee from hard drives. *Etzion v. Etzion*, 19 M3d 1102(A), 859 NYS2d 902 (S.Ct., Nassau Co., 2005, Stack, J.)

B. Access Denied

1. Access to law firm's computer for electronic discovery of billing records and documents related to spouses' estate planning properly was denied by firm, since records had no bearing on validity of prenuptial agreement, in executors' suit to determine widow's right of election renounced by each spouse in prenuptial agreement, and widow had already been provided with hard copies of estate planning file. (*In re Maura*, 17 M3d 237, 842 NYS2d 851 [Surr. Ct., Nassau Co., 2007]]

2. *R.C. v. B.W.,* NYLJ, 4/23/08, p.26 col.1 (S.Ct., Kings Co., 2008) – denied "fishing expedition" into wife's computer where information sought was not limited and "particularly" did "not seek financial documents, records, billing statements or bank statements".

3. *Melcher v. Apollo Med. Fund Mgmt.*, 52 AD3d 244, 859 NSY2d 160 (1st Dept. 2008 -- In addressing the issue of "cloning" a computer hard drive, the court held that: "In view of the absence of proof that plaintiff intentionally destroyed or withheld evidence, his assistant's testimony that she searched his computers, and the adequate explanation for the nonproduction of two items of correspondence, the court improperly directed the cloning of plaintiff's computer hard drives."

C. Safeguards

1. The party from whom electronic discovery is sought should be required to produce material stored on a computer so long as the party being asked to produce the material is protected from undue burden and expense and privileged material is protected. *Lipco Electrical Corp. V. ASG Consulting Corp.*, 4 M3d 1019 (S.Ct., Nassau Co., 2004, Austin, J.)

D. Authentication

1. Where wife found on a family computer a file entitled "MY LIST", which depicted the husband's sexual encounters with numerous women, and testified that it was similar to a notebook she had discovered in the husband's handwriting giving similar accounts, which notebook disappeared, court held that "Plaintiff's testimony of the source of the document as a file in the family computer was sufficient to identify what it was." *Stafford v. Stafford*, 641 A.2d 348 (Vt. 1993)

XVI. TELEPHONE CONVERSATION RECORDINGS IN COURTROOM

A. CPLR 4506 – Eavesdropping statute

B. Vicarious Consent on behalf of minor

1. Peo. v. Badalamenti, 27 NY3d 423, 34 NYS3d 360 (2016)

a. Vicarious Consent Doctrine applied to NY's Eavesdropping Statute (Penal Law §202.05)

b. If a parent or guardian has a good faith, objectively reasonable basis to believe that it is necessary, in order to serve the best interests of his or her minor child, to create an audio or video recording of a conversation to which the child is a party, the parent or guardian may vicariously consent on behalf of the child to the recording. A parent or guardian who is acting in bad faith or is merely curious about his or her

minor child's conversations cannot give lawful vicarious consent to their recording, for purposes of the eavesdropping statute. A trial court should consider all objections to the relevance of portions of the recording, and if possible, it should do so before a recording is played to the jury, so that parts that have no relevance do not become public by inclusion in a trial.

c. The Court followed the federal case of *Pollack v. Pollack* (6th Cir.) and the New York case of *Peo. v. Clark*, 19 Misc3d 6). In *Clark*, an autistic child got off the bus with bruises so the mother put a tape recorder in the child's backpack, leading to the arrest of the bus matron.

d. As to the criticism that the ruling will impair the autonomy of a child, the court quoted a Supreme Court of the United States case, stating that: "traditionally at common law, and still today, unemancipated minors lack some of the most fundamental rights of self-determination… They are subject, even as to their physical freedom, to the control of their parents or guardians."

XVII. EVIDENTIARY HURDLE – PREJUDICE

Is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or should otherwise be excluded under Federal Rule 403.

XVIII. COMPUTER INSPECTION PROTOCOL

Schreiber v. Schreiber, NYLJ, 7/19/2010 NYLJ 17, (col. 1), S.Ct., Kings Co., Thomas, J. 904 NYS2d 886 - Where plaintiff wife moved for an order directing the hard drive disk of defendant husband's office computer be confiscated and/or permitted to be copied in its entirety, alleging that defendant concealed his income and assets to avoid paying the fair share of marital income and assets earned and acquired during the couples' 30 year marriage, the court found that plaintiff was not entitled to an unrestricted turnover of the computer hard drive disk. It found the request was overbroad as it sought general, and unlimited in time, access to the entirety of defendant's business and personal data stored on his office computer. Thus, it denied plaintiff's motion to compel production of the hard drive, with leave to renew provided the renewal application contained a detailed discovery protocol that would protect privileged and private material. The court further provided a proposed list of items such protocol should contain, including:

1. Discovery Referee: The parties will have until the renewal deadline to agree on an *attorney referee, preferably someone with some technical expertise in computer science,* to be appointed pursuant to CPLR 3104 (b) to

supervise discovery (the referee).[FN10] If the parties fail to agree on a referee before the renewal deadline, they will submit two names each to the court (along with a summary of the proposed referee's qualifications, not to exceed one page, and hourly rate), and the court will select a referee from among the candidates submitted.

2. Forensic Computer Expert: The parties will have until the renewal deadline to agree on a forensic computer expert who will inspect and analyze the clone (the expert). If the parties fail to agree on an expert before the renewal deadline, they will submit two names each to the court (along with a summary of the proposed expert's qualifications, not to exceed one page, and the expert's fee structure), and the court will select an expert from among the candidates submitted. The expert will execute a *confidentiality agreemen*t (to be agreed upon by the parties) governing non-disclosure of the contents of the clone and its re-delivery to defendant's counsel after completion of electronic discovery.

3. File Analysis: *The expert will analyze the clone for evidence of any download, installation, and/or utilization of any software program, application, or utility which has the capability of deleting or altering files so that they are not recoverable (a drivewiping utility). The expert will then (i) extract from the clone all live files and file fragments, and (ii) if the files on the clone have been deleted or altered using a drive-wiping utility, will also recover all deleted files and file fragments*.

4. Scope of Discovery: Plaintiff will list the keywords and other searches she proposes to have the expert run on the files and file fragments, subject to a reasonably short time frame (to be agreed upon by the parties) in which such files or file fragments were created or modified. Plaintiff is cautioned that she should narrowly tailor her search queries so as to expedite discovery and reduce the costs of litigation to the parties. To illustrate, a search query for all documents with an.xls (Microsoft Excel) extension, created or modified within a three-year period preceding the commencement of this matrimonial action, will not be permitted.

5. First-Level Review: The expert will run the keywords or other searches on all of the extracted files and file fragments. After performing searches, the expert will export to CDs or DVDs a copy of the native files and file fragments which were hit by such searches, and will deliver such media to defendant's counsel to conduct a privilege review. An exact copy of the media delivered to defendant's counsel will be contemporaneously delivered by the expert to the referee. The expert will also concurrently deliver to the referee and to counsel for both parties a report (i) detailing the results of its searches, (ii) listing the file types for all files hit by the searches, with the file extensions and number of files for each, and (iii) stating whether or not it found evidence of the use of a drive-wiping utility.

6. Second-Level Review: Within twenty days after delivery of the media containing the extracted files and file fragments, defendant's counsel will

deliver to plaintiff's counsel in electronic format (to be agreed upon by the parties) all non-privileged documents and information included in the extracted files and file fragments, together with a privilege log which identifies each document for which defendant claims privilege and describes the nature of the documents withheld (but without revealing information which is itself privileged), so as to enable plaintiff to assess the applicability of privilege.

7. Discovery Disputes: The referee will resolve any disputes concerning relevancy and privilege. Subject to the parties' agreement, the referee's determination will be final.

8. Cost Sharing: All costs for the expert will be borne by plaintiff, subject to any possible reallocation of costs at the conclusion of this action. Plaintiff will indicate if she is willing to bear any other discovery-related costs and, if so, specify her proposed share.

9. Discovery Deadline: The parties should agree to a fast-track discovery schedule, subject to an outside ninety-day deadline within which discovery should be completed.

10. Retention of Clone: The discovery referee will keep the clone until the action is concluded, at which time the clone will be returned to defendant's counsel for disposal.

11. Counsel for parties should discuss and seek to memorialize protocols before engaging in motion practice.

XIX. ISSUE OF TRANSMISSION; USE OF ADVERSE PARTY'S E-MAILS

A. *Gurevich v. Gurevich*, 24 M3d 808, 886 NYS2d 558 (S.Ct.,, Kings Co., 2009, Sunshine, J.) -- A party to a matrimonial action has the right to access and utilize the email account of the estranged spouse whom she no longer resides with and obtain copies of emails in his email account. Such action does not constitute illegal "eavesdropping" pursuant to Penal Law §250.00 which requires unlawfully intercepting or accessing electronic mail. That section prohibits individuals from intercepting communications going from one person to another. Here, the emails were not "in transit" but was stored in an email account, and thus there was no interception, and the emails could not be suppressed pursuant to CPLR §4506[1]. Wife was using husband's emails to show a scheme by husband to hide his income. See also, *Peo. v. Thompson*, 51 M3d 693, 28 NYS3d 237 (2016)

B. 18 USC §§ 2511 and 2520 prohibit only intercepts that are contemporaneous with transmission, i.e., the intercepted communication must be in transit, not in storage (*see, Wesley Coll. v Pitts,* 974 F Supp 375, 385-386 [D Del], *affd* 172 F3d 861 [3d Cir]). *Hudson v Goldman Sachs & Co., Inc.*, 283 AD2d 246, 247, 725 NYS2d 318 (1st Dept. 2001)

XX. SERVICE BY E-MAIL

A. Where service of summons and complaint impractical by conventional means, an alternative method of service pursuant to CPLR 308(5) is, under the facts of the case, by e-mail which was reasonably calculated to give defendant notice of the action. *Synder v. Alternate Energy Inc.,* 19 M3d 954, 857 NYS2d 442 (Civ. Ct., NY Co., 2008)

B. A wife was permitted to serve her husband with a summons with notice by sending it to him through Facebook private messenger after she made good faith attempts to find out where he was, and she submitted an affidavit with copies of exchanges attached that she had with the husband through Facebook. However, since litigants are not permitted to serve each other, wife's attorney was authorized to log into the wife's Facebook account and send the husband a message, first identifying himself as a lawyer, and then sending a copy of the summons with notice. *Baidoo v. Blood-Dzraku*, 48 Misc3d 309 (NY Co., 2015, Cooper, J.)

C. The court denied wife's request for permission to personally serve her husband with a summons for divorce by Facebook where the wife did not show that her husband actually used this Facebook paid for communicating. There was no sworn statement from the wife saying that she had communicated with the husband through this Facebook page, nor did she submit a copy of the exchanges she told her lawyer she had had with defendant through Facebook. *Qaza v. Alschalabi*, 54 Misc3d 69 (Kings Co., 2016, Sunshine, J.) -

XXI. HEARSAY (OR EXCEPTION)

A. Admitted for truth? - When proffering emails as evidence, parties have to confront the hearsay rule, just as they would with hard-written correspondence. If the email is being admitted for its truth, it is barred by the hearsay rule unless an exception is present; and if it is not being offered for the truth, the hearsay rule is inapplicable.

B. Computer Stored Records v. Computer Generated Records

1. Computer stored records – input of humans kept in electronic form

2. Computer generated records – output of a program that processes input following a defined algorithm; does not contain human statements. Hearsay inapplicable as not dependent upon statement or observation of a human declarant.

3. *People v Stultz*, 284 AD2d 350, 351, 726 NYS2d 437 (2d Dept. 2001) - A detective's testimony that he ascertained the telephone number of the telephone in the park where the crime occurred by dialing “953”, generating a recorded response, was properly admitted, and was not inadmissible hearsay since it was not the repetition of a human observation.

C. Some Hearsay Exceptions to Consider

1. Admission of party-opponent - An e-mail forwarded by a party-opponent may be deemed an adoptive admission of the e-mail contents. (See, *Sea-Land Serv. Inc. v. Lozen Int’l. LLC*, 285 F3d 808 [9th Cir. 2002]

2. State of Mind

a. E-mails introduced in libel action in order to establish their effect upon plaintiff, as opposed to the truth of their content, did not constitute inadmissible hearsay. *Rombom v Weberman*, 2002 NY Slip Op 50245(U), 2002 WL 1461890 [Sup Ct June 13, 2002] affd, 309 AD2d 844, 766 NYS2d 88 [2d Dept. 2003]; see also, *Arch-Bilt Corp. v. Interboro Mut. Indem. Ins. Co.*, 119 AD2d 713, 501 NYS2d 127 [2d Dept. 1986])

3. Business Record Rule (CPLR 4518)

a. *Secretary of the Dept. of Housing and Urban Dev. v. Torres,* 2 M2d 53, 774 NYS2d 245 (App. Term, 2d Dept. 2003) – DSS computer printout showing the issuance of rent subsidy checks were admissible under the business records exception.

b. Business record exception is sufficiently broad to admit *computer printouts*. (*Ed Guth Realty, Inc.* v. *Gingold*, 34 NY2d 440, 358 NYS2d 367 (1974); see also, *Briar Hill Apts Co.* v. *Teperman*, 568 NYS2d 50 (1st Dept., 1991); *Peo. v. Weinberg*, 183 AD2d 932, 586 NYS2d 132 (2d Dept., 1992) (Computer tapes made in regular course of business where data is entered into the computer at the time of each transaction qualified as an admissible business record); *F.K. Gailey Co., Inc. v. Wahl*, 262 AD2d 985, 692 NYS2d 563 (4th Dept., 1999) (Computer printouts of outstanding amounts due plaintiff was properly admitted as a business record as the data was stored in the regular course of business); *Federal Express v. Federal Jeans*, 14 AD3d 424, 788 NYS2d 113 (1st Dept. 2005) (Computer generated records admissible upon showing that information was entered in regular course of business)

c. Introduction of computer printouts of electronic business records if the underlying data were stored in the regular course of business. See, e.g., *F.K. Gailey Co. v. Wahl*, 1999, 262 AD2d 985, 692 NYS2d 563 (4th Dep't); *In re Thomma*, 1996, 232 AD2d 422, 648 NYS2d 453 (2d

Dep't), as they are “summaries” of voluminous records, an exception to the best evidence rule. (*Ed Guth Realty, Inc. v. Gingold*, 1974, 34 N.Y.2d 440, 451-52, 358 NYS2d 367, 374, 315 N.E.2d 441, 446)

d. cf. *American Express Bank, FSB v. Zweigenhaft*, 38 M3d 1218(A), 2013 N.Y. slip Op. 50137(U) – Credit card statements not deemed to fall within the business records exception absent sufficient proof that everyone in the chain of information – from the vendor all the way through the generator of the statements – must be acting within the course of regular business conduct.

4. Present Sense Impression; Excited Utterance

a. Emails admitted into evidence where they explain the event in question shortly after it occurred. The key issue on admissibility is whether the statement was substantially contemporaneous with the event in question. Fed. Rules of Evidence 803(1).

5. NY’s common law public records exception - *Miriam Osborn Memorial Home Assn., v. Assessor of the City of Rye*, 9 Misc.3d 1019, 800 NYS2d 909 [S.Ct., Westchester Co., 2005] (Printout from webpage of government website containing real property sales data admissible). Under the common law public documents hearsay exception, “when a public officer is required or authorized by statute or nature of the duty of the office, to keep records or to make reports of acts or transactions occurring in the course of the official duty, the records or reports are admissible in evidence.” [Richard T. Farrell, Prince, Richardson on Evidence § 8-1101 (11th ed. 1995); See also: *People v. Hudson,* 237 AD2d 943, 655 NYS2d 219 (4th Dept.1997)

XXII. E-MAILS; STATUTE OF FRAUDS

A. *Al-Bawaba.com Inc. v. Nstein Technologies Corp.,* 19 M3d 1125(A), 862 NYS2d 912 (S.Ct., Kings co., 2008, Demarest, J.) – The note or memorandum requirement of the Statute of Frauds may be pieced together out of separate writings, some signed, and some unsigned, provided that they clearly referred to the same subject matter or transaction. The signature of the party on the e-mail constituted a “signed writing” under the Statute of Frauds and the sender manifested his intention to authenticate the e-mail for the purpose of the statute of frauds by typing his name at the conclusion of the e-mail referencing the parties’ contractual agreement.

B. The e-mails exchanged between counsel, which contained their printed names at the end, constitute signed writings (CPLR 2104) within the meaning of the statute of frauds (*see Stevens v Publicis S.A.*, 50 AD3d 253,

255-256 [2008], *lv dismissed* 10 NY3d 930 [2008]), and entitle plaintiff to judgment (CPLR 5003-a [e]). *Williamson v Delsener*, 59 AD3d 291, 874 NYS2d 41 [1st Dept. 2009]; *Jimenez v. Yanne*, 152 AD3d 434, 55 NYS3d 652 (1st Dept. 2017)

C. While e-mails may satisfy the Statute of Frauds, in case at bar, right of first refusal proposed in an e-mail was not enforceable under Statute of Frauds, where there was no meeting of the minds, as plaintiff never accepted the offer, and the parties' subsequent oral agreement was based on different price term. *Naldi v Grunberg*, 80 AD3d 1, 908 NYS2d 639 (1st Dept.2010)

XXIII. WEBSITE STATEMENT AS NON-HEARSAY – VERBAL ACT

A. Example: in a breach of warranty case, customer relies upon assurance posted on defendant's website in purchasing a product; the assurance is a warranty (has legal significance).

XXIV. PRIVILEDGED COMMUNICATIONS AND ELECTRONIC COMMUNICATIONS

A. CPLR §4548. Privileged communications; electronic communication thereof.

1. "No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication."

XXV. THIRD PARTY TRANSMISSION

A. *Green v. Beer,* NYLJ, 9/16/10, p.44 col.1, SDNY, Wood, J. - Plaintiffs did not waive the attorney client privilege as to e-mails their lawyer sent to their son, who served as agents for his parents and whose technological assistance helped his parents receive timely e-mail communications. Plaintiffs had a reasonable expectation that the e-mail communications would remain confidential, and the son served as a necessary conduit in delivering the attorney's confidential e-mails to plaintiff. The involvement of a person who plays a necessary role in the delivery of an electronic communication does not constitute a waiver of privilege.

XXVI. PRIVILEGE LOG

A. *Rosewell Park Cancer Institute Corporation v. Sodexo America*, 68 AD3d 1720, 891 NYS2d 827 (4th Dept. 2009) – A claim of protection from discovery because of attorney-client privilege, work product privilege or as material prepared for litigation is necessarily a fact-specific determination, often requiring in camera review. A privilege log should be submitted to court setting forth the author of each e-mail document and attachment, the person to whom each document was sent, the date of transmittal and a description of each document, with an affidavit explaining the claim of privilege. There is nothing in the law governing attorney-client privilege that precludes the privilege from attaching to client communications made in response to oral requests by attorneys and the same reasoning applies when counsel asks high level corporate officers to have lower level officers or assistants gather facts and information incident to the provision of legal advice.

B. CPLR 3122(b) - "[w]henever a person is required ... to produce documents for inspection, and where such person withholds one or more documents that appear to be within the category of the documents required ... to be produced, such person shall give notice to the party seeking the production and inspection of the documents that one or more such documents are being withheld. This notice shall indicate the legal ground for withholding each such document, and shall provide the following information as to each such document, unless the party withholding the document states that divulgence of such information would cause disclosure of the allegedly privileged information: (1) type of document; (2) the general subject matter of the document; (3) the date of the document; and (4) such other information as is sufficient to identify the document".

C. Federal Rules of Civil Procedure 26(b)(5) – A party resisting disclosure based upon privilege must provide complete identifying information, date, type of document, and subject matter in a privilege log at the time the party responds to discovery. To overcome privilege log challenges, the party withholding the documents must ensure that each corresponding log entry contains enough information to satisfy every element of the privilege designation.

SOCIAL MEDIA AND ETHICAL CONSIDERATIONS

I. CLIENT READING SPOUSE'S EMAIL

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

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

II. ADVICE TO "TAKE DOWN" A POSTING

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

1. Can have content taken down but it must be preserved so if asked for in discovery, it can be produced. Otherwise social media content can't be deleted.

2. There may be a duty to preserve "potential evidence" in advance of any request for its discovery. *Voom HD Holdings LLC v. EchoStar Satellite LLC*, 93 AD3d 33 (1st Dept. 2012) ("Once a party reasonably anticipates litigation, it must, at a minimum, institute an appropriate litigation hold to prevent the routine destruction of electronic data.")

3. Permissible for an attorney to review what a client plans to publish on a social media page in advance of publication, to guide the client appropriately, including formulating a corporate policy on social media usage. An attorney may not erect or facilitate the client's publishing of false or misleading information that may be relevant to a claim or participate in the creation or preservation of evidence when the lawyer knows or it is obvious that the evidence is false. RPC 3.4 (a) (4); NYCLA Ethics Opinion 745 (2013)

III. "FRIENDING" ON SOCIAL NETWORKING WEBSITES

A. Assn. of Bar of City of New York, Ethics Opinion 2010-2

1. A lawyer or a lawyer's agent may not attempt to gain access to a social networking website under false pretenses.

2. An attorney or her agent may use her real name and profile to send a "friend" request to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request. Ethical boundaries are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all of the ethical requirements.

a. Opinion refers to the fact that it is "not difficult to envision a matrimonial matter in which allegations of infidelity may be substantiated in whole or part by postings on a Facebook wall."

3. So long as the attorney does not engage in the direct or indirect use of affirmatively deceptive behavior to "friend" a witness, such as creating a fraudulent profile that falsely portrays a lawyer or agent as a long–lost classmate, a prospective employer or a friend of a friend. The attorney has an ethical obligation to disclose his or her real name.

B. cf. N.Y. County Lawyers' Association, Ethics Opinion 737

1. Nongovernment attorneys may… Ethically supervise non-attorney investigators employing a limited amount of dissemblance in some strictly limited circumstances where:… (b) the dissemblance is expressly authorized by law; and (ii) the evidence sought is not reasonably available through other lawful means; and (iii) the lawyer's conduct and the investigators' conduct that the lawyer is supervising do not otherwise violate the code (including, but not limited to DR 7–104, the "no contact" rule) or applicable law; and (iv) the dissemblance does not unlawfully or unethically violate the rights of third parties." (Note "dissemblance", in this content context, includes concealment or misstatement of identity and purpose in the process of evidence gathering.)

C. NYCLA Formal Opinion 750 (2017) – "Adding" an adverse party or adverse witness on Snapschat

1. A lawyer is prohibited, either directly or indirectly, from using deceptive means to access the restricted electronic social media maintained by an adverse party or witness. A lawyer is prohibited, directly or through his or her agent, from seeking to add the adverse party or witness as a "friend" because there is no ability simultaneously to inform the Snapshot user of the lawyer's role in the pending adverse proceeding and the reason the lawyer is seeking access, such that seeking to add the adverse party or witness would result in deception by omission.

D. Unethical v. Inadmissible

1. Radder v CSX Transp., Inc., 68 AD3d 1743, 1743-1745, 893 NYS2d 725 [4th Dept 2009] - Generally, "absent some constitutional, statutory, or decisional authority mandating the suppression of otherwise valid evidence, such evidence will be admissible [in a civil action] even if procured by unethical means" (*Heimanson v Farkas*, 292 AD2d 421, 422 [2002]; *see Nordhauser v New York City Health & Hosps. Corp.*, 176 AD2d 787, 791 [1991]; *see generally, Sackler v Sackler*, 15 NY2d 40, 43-44 [1964]).

IV. DELIVERING CLIENT FILES TO CLIENT

A. NYSBA Ethics Opinion 1142 (1/5/18) – Maintenance of files in Electronic Form

1. Where a lawyer keeps client files received in electronic form in that form and a former client requests a copy of the file in paper form, the lawyer must take reasonable measures to deliver the electronic documents in a form in which the client can access them, but the lawyer may charge the client the reasonable fees and expenses incurred in printing out and delivering a paper copy.

2. Except for documents such as wills, deeds, contracts, and promissory notes or other documents whose legal effect or evidentiary value may be impaired by destroying originals, lawyers are permitted to maintain electronic copies of documents in lieu of paper originals.

B. NYSBA Ethics Opinion 1164 (3/21/19) – Returning Client Files without Keeping a Copy

1. Compliance with the terms of a settlement reached by a former client provides a legitimate reason to comply with that former client's request to destroy the client–owned documents in a lawyer's possession, whether written or digital. The lawyer may condition deletion of the file on

obtaining a release and a simple hold harmless clause from the former client, and may maintain an inventory of the filenames, sizes, and dates for data supplied by the former client to the lawyer during the representation and maintained in the lawyer's files.

V. METADATA

A. Metadata is data hidden in documents that are generated during the course of creating and entering a document.

B. Use of Metadata – Conflicting Opinions

1. Prohibition

a. NYSBA Comm. on Professional Ethics, Op. 782 (2004) - attorneys receiving documents with metadata "have an obligation not to exploit an inadvertence or unauthorized transmission of client confidences or secrets", and using computer technology to intentionally mine metadata contained in an electronic document would constitute "an impermissible intrusion on the attorney – client relationship (citing NYSBA Comm. on Professional Ethics, Op. 749 [2001])

b. NY County Lawyers Assn. Professional Etrhics Comm., Op. 738 (2002) – "[a] lawyer who receives from an adversary electronic documents that appear to contain inadvertently produced metadata is ethically obligated to avoid searching the metadata in those documents."

2. No Prohibition

a. ABA Comm. on Ethics and Professional Responsibility, Formal Ruling 06-442 – A lawyer is not prohibited from extracting metadata intentionally.

VI. JUDICIAL USE OF ELECTRONIC SOCIAL MEDIA

A. ABA Model Code of judicial Conduct, Formal Opinion 462 (2/21/13)

1. As judges are barred from endorsing or opposing candidates for public office, collecting a "like" button on political campaign sites could be perceived as an ethics violation.

2. Judges should not form relationships with persons or groups that may convey an impression that these people and entities are in a position to influence a judge,

3. Judges should take care to avoid comments or interactions that may be interpreted as ex parte communications concerning pending matters and should avoid using social networking sites to obtain information about matters before them.

4. When a judge knows that a party, a witness, or a lawyer appearing before the judge has an electronic social media connection with the judge, the judge should be mindful that such connection may give rise to the level of social relationship or the perception of relationship that requires disclosure or recusal.

B. Independent Internet Research

1. "We also caution the Justice that his independent internet investigation of the plaintiff's standing that included newspaper articles and other materials that fall short of what may be judicially noticed, and which was conducted without providing notice or an opportunity to be heard by any party…was improper and should not be repeated." *HSBC Bank USA, N.A., v Taher*, 104 AD3d 815, 962 NYS2d 301 (2d Dept. 2013)

2. ABA Model Code of Judicial Conduct, Formal Opinion 478 (2017) – Finding "adjudicative facts" about a case online is generally banned. However, a judge is allowed to go online for facts that are subject to judicial notice because they are generally known and not subject to reasonable dispute. Adjudicative facts concern the immediate parties, including who did what, where, when, how and with what motive or intent.

C. A judge who receives a social media message from the victim's relative that contain substantive discussion of the case must disclose the ex parte communication to all parties. OCA Judicial Ethics Opinion 17 – 53 (May 4, 2017)

AUTHENTICATION

I. AUTHENTICATION - WEBSITES AND SOCIAL MEDIA

A. The foundational requirements for authenticating a screenshot from a social media site like Facebook are the same as for a printout from any other website. Basically, the proponent must offer foundational testimony that the screenshot was actually on the website, that it accurately depicts what was on the website, and that the content is attributable to the owner. (*Lorraine v. Market Am. Ins. Co*., 241 F.R.D. 534 (D.Md.2007)) Some courts require the website owner to provide the necessary foundation to authenticate a page from a website. The more liberal courts have held that a printout from a website may be authenticated by a visit to the website. What is required is that the depiction accurately reflects the content of the website and the image of the page on the computer and from which the screen shot was made. A screen shot from a recognized corporation, such as a bank or credit card company generally causes less concern that a personal blog posted where a non-owner can more easily manipulate the content. Information from government websites are deemed self-authenticated if the proponent establishes that the information is current and complete.

B. Suggested Methods of Authorization

1. Testimony from the purported creator of the social network post and related postings;
2. Testimony from persons who received the messages;
3. Testimony about the contextual clues and distinctive aspects in the messages themselves tending to reveal the identity of the sender;
4. Testimony regarding the account holders exclusive access to the originating computer and social media accounts;
5. Expert testimony concerning the results of the search of the social media account holder's computer hard drive;
6. Testimony directly from the social networking website that connects the establishment of the profile to the person who allegedly created and also connects the posting sought to be introduced to the person who initiated it; and
7. Expert testimony regarding how social network accounts are accessed and what methods are used to prevent unauthorized access.

C. Claim of Alteration

1. 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.

2. *U.S. v. Safavian*, 644 F.Supp.2d 1 – "The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents)."

D. Foundations

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

2. Assuming such a witness as above is not available, the proponent can have a witness testify that the witness visited the social media site at issue, read the information there that is reflected in the proposed printout exhibit, remembers the contents of the social media site, and can identify the proposed printout exhibit as accurately reflecting the posting that he or she saw from the social media site. (Similar to the method used authenticating of photograph or other demonstrative exhibit)

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

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

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

6. Whether the person has shared his or her social media password with other people. Whether there is a photograph of the persons or the profile page identifies a person to whom the proponent wishes to attribute the posting.

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

Steps:
(1) Proof that the witness visited the website.
(2) When the website was visited.
(3) Establish that the website was current as opposed to stale sites. For example, postings reflect current information, dates, etc.
(4) Establish how the site was accessed – Google search and followed the links; Internet Explorer, etc.
(5) Description of the website access – identify material on the website including names, addresses, logos, phone numbers, etc.
(6) Recognition of the website based on past visits
(7) Proof that the screen shot was printed from the website and the date and time the screen shot was captured
(8) Proof that the screenshot in the printout is the same as what the witness saw on the computer screen.
(9) Proof that the printout was not altered or modified from the image on the computer.

SAMPLE QUESTIONS – FACEBOOK PAGE

Q: Are you familiar with the social media website Facebook?
A: Yes.
Q: How are you familiar with it?
A: I have been using it 4 to 5 times per week for the last 3 years.
Q: Generally speaking, what you do with the social media site?
A: I generally keep up with my friends and what they are doing and special things in their lives.
Q: What is a Facebook friendship?
A: You are permitted to follow certain chosen friends.
Q: How is a Facebook friendship created?
A: You invite someone to be your friend and if the person accepts you become Facebook friends.
Q: Is Joan Smith your Facebook friend?
A: Yes.
Q: What is a Facebook wall?
A: This is an area where someone has personal information open only to friends.
Q: How you access someone's Facebook wall?
A: You click their profile on the website.
Q: What type of information is found on Joan Smith's wall?
A: Personal information such as special events, pictures, employment, where she lives, etc.
Q: Have you ever visited Joan Smith's wall?
A: Many times.
Q: Have you done so recently?

A: Actually, I did last Thursday.
Q: What did you see on our wall?
A: I saw a picture of her and my husband with their arms around each other at what appeared to be a party, and another picture at the same place where they were kissing.
Q: Did you print a copy of the pictures you saw?
A: Yes.
Continue with identification of the printout in same manner as with email or text message.

II. JUDICIAL NOTICE OF INFORMATION ON WEBSITES

A. "The court's computerized records, which were not included in the record but of which we take judicial notice show that in accordance with the warning in the court's scheduling notice dated November 23, 2004, admittedly received by plaintiff's attorney, the action was dismissed on March 2, 2005 pursuant to 22 NYCRR 202.27 when plaintiff failed to appear for a pre-note of issue conference." *Perez v. New York City Hous. Auth.*, 47 AD3d 505, 850 NYS2d 75 (1st Dept. 2008)

III. OFFICIAL GOVERNMENT WEBSITES

A. Federal Rules of Evidence §902(5) - website operated by a government agency is self-authenticating.

B. State Department of Insurance for corporate presence in county (*N.Y.C. Medical and Neurodiagnostic, P.C. v. Republic Western Ins. Co.*, 3 Misc3d 925, 774 NYS2d 916 [Civ. Ct. NY 2004], *revd on other grounds*, 8 Misc3d 33, 798 NYS2d 309 [App. T. 2d Dep't. 2004]

C. Surgeon General report for dangers of second-hand smoke (*DeMatteo v. DeMatteo*, 194 Misc 2d 640, 749 NYS2d 671 [Sup. Ct. NY 2002][Julian, J.]

D. Secretary of State for "entity information" for plaintiff as to its principal place of business (*Tener Consulting Services, LLC v FSA Main St., LLC*, 23 Misc 3d 1120(A), 886 NYS2d 72, [Sup Ct 2009].

E. "However, the Court has learned (from its own research) that plaintiff is still registered with the Secretary of State as the "Chairman or Chief Executive Officer" of Venezia. The Court rather than counsel for defendant uncovered this evidence by a quick review of the official website of the New York Secretary of State. While certainly unusual, the Court is

allowed to take judicial notice of this matter of public record. *See Brandes Meat Corp. v. Cromer,* 146 AD2d 666, 537 NYS2d 177 (2d Dept.1989); *Chasalow v. Board of Assessors of County of Nassau.* 176 AD2d 800, 575 NYS2d 129 (2d Dept.1991). The Court informed the parties that it would be taking judicial notice of this fact at a Court conference." *Munaron v. Munaron*, 21 Misc3d 295, 862 NYS2d 796 [S.Ct.. Westchester Co. 2008 Jamieson, J.]

F. U.S. Naval Observatory for time of sunrise (*United States v. Bervaldi*, 226 F.3d 1256, 1266, n. 9 [11th Cir. 2000])

G. Federal Reserve Board for prime interest rate (*Levan v. Capital Cities ABC, Inc.*, 190 F.3d 1230, 1235, n. 12 [11th Cir. 1999])

H. National Personnel Records Center for records of retired military personnel (*Denius v. Dunlap*, 330 F.3d 919, 926 [7th Cir. 2003])

I. Department of State (NYS) online search results for whether physician was licensed to practice medicine in NYS (*Proscan Radiology of Buffalo v. Progressive Cas. Ins. Co.***,** 12 M3d 1176(A), 820 NYS2d 845 (Civil Ct., NY, 2006) :

> "On the other hand, there are specific exceptions to the hearsay rules with regard to documents maintained by governmental agencies given the inherent reliability of such documents. It would seem that the fact that these documents were obtained by downloading them from the government's website rather than through the physical receipt of them from the governmental agency itself is somewhat of a distinction without a difference. In this regard, the Court notes that the Appellate Division, Second Department, has recently cited with approval a number of cases in which trial courts have taken judicial notice of documents that the courts themselves have downloaded from government websites (*see Kingsbrook Jewish Med. Ctr. v. Allstate Ins. Co.,* 2009 N.Y. Slip Op 000351, 871 NYS2d 680 [2d Dept 2009], *citing Munaron v. Munaron,* 21 Misc3d 295 [Sup Ct Westchester County 2008]; *Parrino v. Russo,* 19 Misc3d 1127[A], 2008 WL 1915133 [Civ Ct Kings County 2008]; *Nairne v. Perkins,* 14 Misc3d 1237[A], 2007 WL 656301 [Civ Ct Kings County 2007]; *Proscan Radiology of Buffalo v. Progressive Cas. Ins. Co.,* 12 Misc3d 1176 [A], 2006 WL 1815210 [Buffalo City Ct.2006]; *see also Bernstein v. City of New York,* 2007 N.Y. Slip Op 50162[U], 14 Misc3d 1225[A] [Sup Ct Kings County 2007]; *Miriam Osborn Memorial Home Assn. v. Assessor of City of Rye,* 9 Misc3d 1019 [Sup Ct Westchester County 2005]). There is every reason to believe that the information that appears on governmental websites is a reasonably reliable reflection of what the hard copies on file with the government show."

J. cf. *Morales v. City of New York*, 18 M3d 686, 849 NYS2d 406 (S.Ct., 2007) - "this Court is not aware that any New York appellate court has passed definitively upon the admissibility as evidence of public records printed from even a New York government website."

IV. PRIVATE OR COMMERCIAL WEBSITES

A. Hospital website for asthmatic conditions and causes (*Gallegos v. Elite Model Management Corp*., 195 M2d 223,758 NYS.2d 777 [Sup. Ct. NY 2003])

B. Trial court abused its discretion in not taking judicial notice of defendant corporation's historical retirement fund earnings posted on its website (*O'Toole v. Northrop Grumman Corp.,* 499 F3d 1218, 1225 [10th Cir. 2007])

C. Mapquest for mileage distance (*In Re Extradition of Gonzales*, 52 FSupp2d 725, 731, n. 12 [Wd La. 1999]; See, CPLR Rule 4511

V. WEBSITE ADMISSIONS

A. *NYC Medical and Neurodiagnostic, P.C. v. Republic Western Ins. Co.*, 3 M3d 925, 774 NYS2d 916 (Civ. Ct., Qns. Co., 2004) - Information posted on corporate party's website constitute admissions, and are encompassed by the admissions exception to the hearsay rule. See, *NYC Medical and Neurodiagnostic, P.C. v. Republic Western Ins. Co.,* 8 M3d 33, 798 NYS2d 309 (App Term) (Trial judge made independent internet investigation to see if defendant was transacting business in NY. "Even assuming the court was taking judicial notice of the facts, there was no showing that the Web sites consulted were of undisputed reliability, and the parties had no opportunity to be heard as to the propriety of taking judicial notice in the particular instance (see, Prince, Richardson on Evidence §20202 [Farrell 11th ed]").

B. Website Statement as non-hearsay – Verbal Act (i.e., breach of warranty case)

VI. AUTHENTICATION - SYSTEM/PROCESS CAPABLE OF PRODUCING RELIABLE/ACCURATE RESULT (FRE 901(B)(9))

A. *U.S. v. Washington*, 498 F.3d 225 (4th Cir. 2007) - computer readout of electronic forensic analysis of defendant's blood sample for drug and alcohol content is admissible if authentic; readout was not hearsay because there was no "declarant" under rule 801 (b).

B. Important for authenticating computer simulations. Generally requires proof of reliability of scientific or technical principles and thus involves a *Daubert* or *Frye* situation. See, e.g. *Ruffin ex rel Sanders v. Bolder*, 809 N.E.2d 1174 [Ill. App. Ct. 2008) (simulation showing force exerted in childbirth)

C. Requires a witness who has personal knowledge to explain how the social media evidence was created or, alternatively, is a qualified expert.

D. Important for authenticating computer simulations

1. Example – Turbo Tax

VII. SELF-AUTHENTICATION (RULE 902)

A. Rule 902(7) allows for self-authentication for documents that bear "inscriptions, signs, tags or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin."

B. *U.S. Equal Employment Opportunity Commission v. E.I. DuPont de Nemours & Co.,* 2004 WL 2347559 (E.D. La. 10/18/04) - "a printout of a table from the website of the United States Census Bureau," which "contained the internet domain address from which the table was printed, and the date on which it was printed," was admissible because it was self-authenticating."

C. Inscriptions, signs, tag, or labels purporting to be affixed in the course of business and indicating ownership, control, or origin are self-authenticating. (FLR 902[7])

1. Example: automatic signature at end of an e-mail

D. Comparison with another properly authenticated e-mail. (*U.S. v. Safavian*, 435 FSupp.2d 36 (D.D.C. 2006))

E. Presumption of authenticity - Documents produced by adverse party as part of discovery in litigation (see, *Indianapolis Minority Contractors Ass'n., Inc. V. Wiley*, 1998 WL 1988826 (S.D. Ind. 5/13/98); *Perfect 10, Inc., 213 F.Supp.2d 1146.*

VIII. EVIDENTIARY HURDLE – RELEVANCE

A. Does the ESI ten to prove or disprove a fact that is of consequence to the trial?

B. FRE 401 – low threshold

1. cf. with issue of weight and credibility [FRE 104(e)]

2. requirement 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.

IX. EVIDENTIARY HURDLE - AUTHENTICATION - GENERALLY

A. Most significant issue for ESI - E-mails, text messages and social media data are subject to the same requirements for authentication as traditional paper documents.

B. Non-testimonial evidence- writings, photographs, recordings – must be authenticated, i.e, the evidence is what it is purported to be. (FRE 901(a))

C. FRE 901(b) identifies ten nonexclusive examples of how authentication can be accomplished.

D. Electronically stored information "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)

1. When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity is much easier to establish. A screen shot won't include metadata or other information that can't be "seen" but which may be critically important to a lawsuit and/or to authenticate the data.

E. General Proposition – anyone with personal knowledge of an electronic mail message, including the sender and recipient, can authenticate

F. Policy - *U.S. v. Safavian*, 644 F.Supp.2d 1 (1009) - "As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead 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."

X. CIRCUMSTANTIAL EVIDENCE AS BASIS FOR AUTHENTICATION

A. Circumstantial Evidence (Fed. Rules of Civil Proc., Rule 901(b)(4)) - offer testimony about the distinctive characteristics of a message when considered in conjunction with the surrounding circumstances.)

1. 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. E-mails and text messages have been admitted based on circumstantial evidence. In *Lorraine*, *supra,* the 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." Fed.R.Evid. 901(b)(4); *United States 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"),

D. E-mails properly authenticated when they included defendant's e-mail address, the reply function automatically dialed defendant's e-mail address as sender, messages contained factual details known to defendant, messages included defendant's nickname, and other metadata. *U.S. v. Siddiqui,* 235 F3d 1318, 1322-23 (11th Cir. 2000)

1. Circumstantial evidence can verify emails just as such evidence authenticates a voice heard over the telephone when the message reveals the speaker had knowledge of the facts that only the speaker would likely know. Here, the emails contain sufficient circumstantial evidence to authenticate defendant Charles and recipient and send as the emails were sent from his alleged account referenced the purchase of the house in question, the family members by name, and other facts showing that the emails were written and received by defendant Charles. *Smith v. Charles,* 37 Misc2d 1229(A), 964 NYS2d 63 (Supreme Court, Kings Co. 2012, Lewis, J.)

2. Objections overruled to exhibits printed from the Internet that were 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." *Perfect 10,*

Inc. v. Cybernet Ventures, Inc. , 213 F.Supp.2d 1146, 1153 – 54 (C.D. Cal. 2001)

E. Consider the e-mail address of the purported sender and the fact that the apparent author would have been familiar with the content of the e-mail.

1. *U.S. v. Safavian*, 435 FSupp.2d 36 (D.D.C. 2006) – emails authenticated by distinctive characteristics including e-mail addresses, the defendant's name, and the contents which contain discussions relating to defendant's work.

XI. AUTHENTICATION – IM COMMUNICATIONS – CIRCUMSTANTIAL EVIDENCE

A. Court properly received, as an admission, Internet 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. (*People v. Pierre*, 41 AD3d 289, 838 NYS2d 546 [1st Dept. 2007]). See also, *People v Clevenstine*, 68 AD3d 1448, 1450-51, 891 NYS2d 511 [3d Dept. 2009] lv to appeal denied, 14 NY3d 799, 925 NE2d 937, 899 NYS2d 133 [2010]:

1. "[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 NY2d 48, 59 [1979]; *see* Prince, Richardson on Evidence § 4-203 [Farrell 11th ed.]).

B. Here, both victims testified that they had engaged in instant messaging about sexual activities with defendant through the social networking site MySpace, 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 disk had been exchanged by users of accounts 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 NY2d 286, 291-293 [1980]; *People v Pierre*, 41 AD3d 289, 291 [2007], *lv denied* 9 NY3d 880 [2007]; *see generally* Zitter, Annotation, *Authentication of Electronically Stored Evidence, Including Text Messages and E-mail*, 34 ALR6th 253)." *People v. Clevenstine*, 68 AD3d 1448, 891 NYS2d 511 (3d Dept. 2009)

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 F3d 140 [2d Cir 2007]; *United States v Tank*, 200 F3d 627 [9th Cir 2000] [a participant to the conversation testified that the print-out of the electronic communication was an accurate representation of the exchange and had not been altered in any significant manner]

1. *State v Roseberry*, 197 Ohio App 3d 256, 2011 Ohio 5921, 967 NE2d 233 [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]). 1095, 988 NE2d 529 (2013)

2. *cf. Peo. v. Givans*, 45 AD3d 1460, 845 NYS2d 665 (4th Dept. 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.

XII. AUTHENTICATION - PERSON WITH KNOWLEDGE

A. Rule 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." (I., 241 F.R.D. 534, 555-56 [D. Md., 2007])

B. *Robmom v. Weberman*, 2002 WL 1461890, 2002 NY Slip Op 50245 (S.Ct., Kings Co., 2002, Jones, J.), affd. 309 AD2d 844, 766 NYS2d 86 (2d Dept. 2003) - E-mails properly admitted where plaintiff testified that the e-mails were a compilation of the many he had received as a result of defendant's directions on their web sites; that he had received them and printed them out on his office computer; and that they are true and accurate copies of what he had received and printed.

C. *U.S. V. Gagliardi*, 506 F3d 140, 151 (2d Cir. 2007) (chat room logs properly authenticated as having been sent by the defendant through testimony from witnesses who had participated in the online conversations.

D. Photographs of text messages between the defendant and the complainant were properly admitted into evidence…The complainant's testimony that the photographs of the text messages fairly and accurately depicted the text message conversation between her and the defendant was sufficient to authenticate the photographs. *People v. Cotto*, 164 AD3d 826, 826–27, 79 NYS3d 535, leave to appeal denied, 32 N.Y.3d 1110, 115 N.E.3d 633, 91 NYS3d 361 (2018)

E. Recorded Conversation

1. Defendant also argues that County Court erred in permitting the People to introduce a private Facebook message in which he made a threat to the second CI, claiming a lack of foundation. "A recorded conversation—such as a printed copy of the content of a set of cell phone instant messages—may be authenticated through, among other methods, the 'testimony of a participant in the conversation that it is a complete and accurate reproduction of the conversation and has not been altered'." (*Matter of Colby II. [Sheba II.]*, 145 AD3d 1271, 1273 [2016], quoting *People v Agudelo*, 96 AD3d 611, 611 [2012], *lv denied* 20 NY3d 1095 [2013]). "The credibility of the authenticating witness and any motive [he or] she may have had to alter the evidence go to the weight to be accorded this evidence, rather than its admissibility" (*People v Agudelo*, 96 AD3d at 611 [citation omitted]). Here, the second CI had been Facebook friends with defendant for two years prior to trial and stated that she knew the message came from defendant's account because an icon of defendant's picture was displayed next to it. She also testified that she had firsthand knowledge of the content of the Facebook message, therefore, she was an appropriate witness to authenticate the message (*see id.* at 612). Additionally, the Facebook message was sufficiently authenticated by the second CI as she explained that the copy shown to her—the same copy that was ultimately admitted as an exhibit at trial—accurately depicted the message that defendant had sent to her (*see Matter of Colby II. [Sheba II.]*, 145 AD3d at 1273). *People v. Shortell*, 155 AD3d 1442, 1444, 66 NYS3d 69, 2017 N.Y. Slip Op. 08410, 2, 2017 WL 5892397 (N.Y. App. Div. 2017), leave to appeal denied, 31 N.Y.3d 1087, 79 NYS3d 109

F. Screenshot

1. We conclude that the father's alleged conduct in allowing a 13-year-old child with no prior experience to operate a boat in that manner "would support a finding of neglect" (*Matter of Bernthon v Mattioli*, 34 AD3d

1165, 1166 [3d Dept 2006]; *see generally* § 1012 [f] [i] [B]), and that the child's statements about the incident were corroborated by the screenshot (*see Matter of Mildred S.G. v Mark G.*, 62 AD3d 460, 462 [1st Dept 2009]), which was properly admitted in evidence at the fact-finding hearing based on the mother's testimony that it accurately represented the father's Facebook page on the date in question and that she had communicated with the father through his Facebook page in the past (*see Matter of Rutland v O'Brien*, 143 AD3d 1060, 1062 [3d Dept 2016]; *see generally People v Price*, 29 NY3d 472, 478-480 [2017]). Montalbano v. Babcock, 155 A.D.3d 1636, 1637, 65 NYS3d 396, 2017 N.Y. Slip Op. 08119, 2, 2017 WL 5506651 (N.Y. App. Div. 2017), leave to appeal denied, 31 N.Y.3d 912, 81 NYS3d 372

XIII. AUTHENTICATION - DISTINCTIVE CHARACTERISTICS

A. Evidence is frequently authenticated circumstantially such as through the distinctive nature of the contents of the messages. *Matter of R.D. (C.L.)*, 58 Misc3d 780 (Fam. Ct., NY Co., 2017). Here, a “screen shot” of text messages sent by a mother to an unknown party agreed to engage in sex for money was authenticated to the following evidence. The father testified that:

1. He observed the incriminating messages on his cell phone and that the screen shot, although he did not personally take it, was an accurate representation of the messages that he saw on the cell phone;
2. The cell phone belong to the mother based on his familiarity with the make, model and color of the cell phone;
3. He has seen the mother use the cell phone many times;
4. When he was visiting his daughters, he picked up the cell phone after running in the mother asked him to handed to her; and
5. The cell phone was password protected, making it unlikely that someone, other than the mother, was able to send the messages sought to be introduced.

B. A document may be authenticated by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Fed.R.Evid. 901(b)(4); *United States 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")

C. E-mails were properly authenticated when they included defendant’s e-mail address, the reply function automatically dialed defendant’s e-mail address as sender, messages contained factual details known to defendant,

messages included defendant's nickname, and other metadata. *U.S. v. Siddiqui,* 235 F3d 1318, 1322-23 (11th Cir. 2000)

1. *U.S. v. Safavian*, 435 FSupp2d 36 (D.D.C. 2006) – emails authenticated by distinctive characteristics including e-mail addresses, the defendant's name, and the contents which contain discussions relating to defendant's work. See also, *Peo. v. Franzese,* 154 AD3d 706, 61 NYS3d 661 (2d Dept. 2018)

2. *Griffin v. Maryland*, 19 A3d 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 as the witness' picture, birth date and location were not sufficiently distinctive characteristics on a MySpace profile page 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 of a likelihood that another user could have created the profile in issue.

In *Griffin*, the court suggested three (3) types of evidence to satisfy the authenticity requirement:

a. Ask the purported creator if he or she created the profile and added the post in question;

b. A search of the computer of the person who allegedly created the profile, examining the hard drive and internal history to determine if it was that person who originated the profile; or

c. Obtain information directly from the social networking website itself to establish who created and posted the relevant information to the profile.

3. *Tienda v. State*, 2010 Tex App Lexis 10031 (2010) - MySpace evidence admitted, the court noting that (1) the evidence was registered to a person with the defendant's *nickname and legal name; (2)* the photographs on the profiles were clearly of the defendant; (3) the profiles referenced the victim's murder and the defendant being arrested and placed on electronic monitoring. The court noted that "this type of individualization is significant in authenticating a particular profile page as having been created by the person depicted in it. The more particular and individualized the information, the greater the support for a reasonable juror's finding that the person depicted supplied the information.

4. Taken together, *Griffen* 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. Contrariwise, if the characteristics are general, courts may require additional corroborating evidence. \

XIV. AUTHENTICATION BY HEADER

A. Often the headers of any email which include electronic address of the sender are enough to authenticate

B. *U.S. v. Safavian*, 644 F.Supp.2d 1 (2009) – Court authenticated any e-mail based on the header.

XV. AUTHENTICATION BY E-MAIL THREAD

A. Authentication can also be established via an e-mail thread. For example, if an e-mail was a reply to someone, the digital conversation could serve as the basis of authentication (*U.S. v. Siddiqui*, 235 F3d 1318 [11th Cir. 2000]).

Sample Q&A

Q. Would you please identify Defendant's Exhibit D.
A: It is a copy of an e-mail I sent to my employer.
Q: When did you send this e-mail?
A: September 9, 2017.
Q: Under what circumstances did you send this e-mail?
A: I was replying to an e-mail my employer sent me earlier in the day.
Q: Do you recognize your employees e-mail address?
A: Yes
Q: What is his e-mail address?
A: Workhard@gmail.com
Q: On the e-mails header does it reflect where this email was sent?
A: Yes.
Q: Where was it sent?
A: Workhard@gmail.com

XVI. AUTHENTICATION BY COMPARISON

A. FRE 901(B)(3) - permits authentication by comparison, i.e., a court can authenticate an e-mail by comparing it to the mails previously admitted.

B. The proponent can then ask the court to take judicial notice of the earlier admitted e-mails.

XVII. AUTHENTICATION BY DISCOVERY PRODUCTION

A. The fact that a party opponent produced e-mails during discovery

can serve as a basis for authentication of the subject e-mails.

B. CPLR 4540-a: Material produced by a party in response to a demand pursuant to article thirty-one of this chapter for material authored or otherwise created by such party shall be presumed authentic when offered into evidence by an adverse party. Such presumption may be rebutted by a preponderance of evidence proving such material is not authentic, and shall not preclude any other objection to admissibility.

C. The production in response to a request for production is inherently an admission of the authenticity of the documents produced. (*John Paul Mitchell Sys. V. Quality Kind Distribs., Inc.*, 106 FSupp2d 462 [S.D.N.Y. 2000])

XVIII. AUTHENTICATION BY TESTIMONY OF SENDER – E-MAIL

STEPS:

1. The electronic address placed on the e-mail is that of the claimed recipient.
2. The purpose of the communication (why it was sent)
3. If applicable, establish that sender receives an earlier e-mail and replied to the earlier email.
4. Establish that the e-mail was actually sent.
5. Establish that the recipient acknowledged receipt or took action consistent with an acknowledgment of receipt.

SAMPLE QUESTIONS – TESTIMONY OF SENDER

Q: Tell the Court what this document is.
A: It is an e-mail I sent my friend Larry.
Q: Do you know Larry's e-mail address?
A: Yes
Q: What is his email address?
A. Larry the Great@optonline.net
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 Larry ever acknowledge the email you sent?
A: Yes, he called me an hour after I sent the email to discuss our dinner plans.

XIX. AUTHENTICATION BY TESTIMONY OF THE RECIPIENT

Steps:
1. Acknowledge receipt of e-mail
2. Establish the electronic address of the sender as being the address indicated on the face of the e-mail.
3. Compare earlier e-mails received by the sender.
4. Identify any logos or other identifying information on the e-mail.
5. Establish whether the e-mail received was a reply to one sent earlier by the recipient**.**
6. Establish any conversations with the sender concerning the communication
7. Establish any actions taken by the sender consistent with the communication

SAMPLE QUESTIONS – TESTIMONY OF RECIPIENT

Q: Please identify this document.
A: It is an e-mail I received from my attorney.
Q: What is the e-mail address of the sender?
A: Dewey@dch.com
Q: Do you recognize any identifying marks on the e-mail?
A: Yes, I recognize the logo of the firm where my attorney works and his phone number is on the e-mail.
Q: When did you receive this e-mail?
A: October 5, 2012.
Q: Had you sent your attorney any e-mails 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 any mail 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 e-mail?
A: Yes, I had a phone conversation with him about 10 minutes after I received the e-mail.
Q: What was the topic of the telephone conversation?
A: It concerned the issue of visitation with my children.

XX. AUTHENTICATION BY CONTENT

A. A proponent of an e-mail may authenticate the e-mail by showing that only the purported author was likely to know the information reflected in the message.

B. Examples:

1. The substantive content of the message might be information only known to the purported sender;

2. If the recipient used a reply feature to respond, the new message will include the sender's original message.

3. If the sender dispatched that message to only one person, its inclusion in the new message indicates that the new message originated with the original recipient.

XXI. AUTHENTICATION BY ACTION CONSISTENT WITH THE MESSAGE

A. After receipt of the e-mail 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.

XXII. AUTHENTICATION - TEXT MESSAGES & IM'S

A. Nature of Text Messages

1. Text messages - Unlike e-mails, typically travel from device to device the same way a cell phone call travels, rather than over the enterprise e-mail servers.

2. Leave footprints that can reveal the general geographic locations of the sender and recipient at the time of dispatch and receipt.

3. Text message content typically only exists in the handheld devices of the sender and recipient, rather than in a server at a workplace. They have a short shelf life and can be destroyed.

4. Text messages are easily lost because they travel from handheld device to handheld device through third parties (the receiving cell phone tower and wireless service) that tend to not retain the message content for more than a few days. By contrast, an e-mail will travel over the Internet from a computer through a server.

B. 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 F3d at 151). Here, there is 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 AD3d 611, 947 NYS2d 96 (1st Dept. 2012) leave to appeal denied, 20 NY3d 1095 (2013)

C. A recorded conversation – such as a printed copy of the content of a set of cell phone instant messages – may be authenticated through, among other methods, the testimony of a participant in the conversation that it is a complete and accurate reproduction of the conversation and has not been altered. The credibility of the authenticating witness and any motor he or she may have had to alter the evidence go to the weight to be accorded this evidence, rather than its admissibility. *People v. Shortell*, 155 AD3d 1442, 66 NYS3d 69 (3d Dept. 2017)

D. Authentication by Testimony of Sender – Steps:

(1) The context of a message – why was it sent, its purpose, etc.
(2) Establish that the number it was sent to was that of the recipient.
(3) Identify a photograph of the actual text that was sent.
(4) Describe the process of taking the photograph – who took it, what camera was used, was it an accurate reproduction of the actual text, etc.
(5) 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.
(6) Establish if there was any responsive text received or any verbal acknowledgment by the recipient in relation to the text sent.

SAMPLE QUESTIONS – TESTIMONY OF SENDER

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: 123–456–7891
Q: Whose numbers 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.

XXIII. AUTHENTICATION BY TESTIMONY OF RECIPIENT

STEPS

1. Have the witness acknowledge recognition of the number, digital signature or name of the person from whom they received a message.
2. Establish the basis of the witness's knowledge of the sender's number (e.g., history of text messages with that person)
3. The context of the text communication (reply to earlier text) or establish the topic that was the subject of the text)
4. If a photograph was used, establish who took the photo, what camera was used, that it was an accurate reproduction of the actual text, etc.
5. 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.

SAMPLE QUESTIONS – TESTIMONY OF RECIPIENT

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 argument you having?
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 various e-mails in chronological order as they exactly 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?
Q: Did you alter or modify in any way the text messages that appear on the transcript?
A: No.

B. Nature of IM's

1. Written communications in electronic format sent from one cell phone to another or some other handheld device.

2. IM's are transmitted via the internet in real time, often through an account provided by an ISP (Internet Service Provider). A screen name or pseudonym is used to identify the sender. Because the sender need only have access to a screen name and password to transmit an IM, some litigants have challenged the admissibility of IMs as being inherently

unreliable. *Peter A. Crusco, "Case Law Continues to Evolve in Admission of Text Messages",* NYLJ, 6/22/2010

C. Authentication

1. Court properly received, as admission, Internet instant message from defendant to victim's cousin; although witness did not save or print 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. (*People v. Pierre*, 41 AD3d 289, 838 NYS2d 546 [1st Dept. 2007]) [email authenticated by circumstantial evidence]]) **[email authenticated by circumstantial evidence]**

2. People v Clevenstine, 68 AD3d 1448, 1450-51, 891 NYS2d 511 [3d Dept. 2009] lv to appeal denied, 14 NY3d 799, 925 NE2d 937, 899 NYS2d 133 [2010]: "[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 NY2d 48, 59 [1979]; *see* Prince, Richardson on Evidence § 4-203 [Farrell 11th ed]). Here, both victims testified that they had engaged in instant messaging about sexual activities with defendant through the social networking site MySpace, 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 disk had been exchanged by users of accounts 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 NY2d 286, 291-293 [1980]; *People v Pierre*, 41 AD3d 289, 291 [2007], *lv denied* 9 NY3d 880 [2007]; *see generally* Zitter, Annotation, *Authentication of Electronically Stored Evidence, Including Text Messages and E-mail*, 34 ALR6th 253).

XXIV. PH0TOGRAPHS; DIGITAL IMAGE FROM WEBSITE

A. *People v. Lenihan*, 30 M3d 289, 911 NYS2d 588 (S.Ct., NY Co., 2010) - Defendant precluded from confronting witnesses with printouts of MySpace photos depicting him in gang clothing because of the easy ability to digitally alter photographs on the computer. Accordingly, proof that a message of a photograph came from a particular account or device without further authenticating evidence, is inadequate proof of authorship or

depiction.

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

C. *People v. Price,* 29 NY3d 472, 58 NYS3d 259 (2017)

1. Court of Appeals addressed the question of "how a party may authenticate a printout of a digital image found on a social media website."

2. The court made it clear that there is no strict rule or formula that must be met in order to have social media communications authenticated in order to be admitted into evidence. However, when a party denies that the actual social media post or picture, frequently offered in the form of a "green shy" quote, was his or hers, there must be sufficient indicia, which may not be difficult to obtain, that the communication came from the author in order to be properly authenticated.

3. The court found the prosecution did not sufficiently authenticate a photograph of the defendant holding a gun which was admitted into evidence during the defendant's criminal trial for robbery. The photograph was obtained from an alleged social media profile of Defendant's on a website. The court noted that there was a failure to proffer evidence that would "actually demonstrate that defendant was aware of – let alone exercise dominion or control over – the profile p. in question." Judge Stein wrote: "… Notably absent with any evidence regarding whether defendant was known to use an account on the website in question, whether he had ever communicated with anyone through the account, or whether the account can be traced to electronic devices owned by him. Nor did the People proffer any evidence indicating whether the account was password protected or assessable by others, whether or non—account holders could pose pictures to the account, or whether the website permitted defendant to remove pictures from his account if he objected to what was depicted therein."

4. In a concurring opinion, Judge Rivera held that to authenticate a photograph obtained from a social media website, there are 2 requirements:

1. In the printout and accurate representation of the webpage; and

2. If the webpage in the dominion and control of the defendant allowing him to post on it.

D. Cell phones

1. Metadata is embedded in photos taken with a phone with GPS technology. Shows the latitude and longitude of where the image was taken. The image travels with the metadata. If no metadata, means the image has been altered as, e.g., Photoshop. The metadata is then gone.

2. With images, check the metadata which you can do yourself or companies can do it. The same is true for videos with cell phones.

XXV. AUTHENTICATION OF YOU TUBE VIDEO

A. Social media video that was admitted into evidence was properly authenticated by certification from provider of the online service, which indicated when the video was posted online, by a police officer who viewed the video at or about the time that it was posted online, and by defendant's own admissions about the video made in a phone call while he was housed at a detention center, as well as by the video's appearance, contents, substance, internal patterns, and other distinctive characteristics. *People v. Franzese*, 154 AD3d 706, 61 NYS3d 661 (2D Dept. 2018)

XXVI. AUTHENTICATION OF YELP REVIEWS

A. In an action for defamation arising out of a commercial landlord-tenant dispute, immediately after plaintiff obtained a Temporary Restraining Order against the defendant, negative Yelp reviews were posted by anonymous accounts. Plaintiff could not reconcile the criticisms of poor service with any existing customers, and plaintiff obtained the IP addresses of the anonymous posts, which were defendant's home and business addresses. At trial defendant objected to the printed anonymous Yelp host being admitted on the basis of improper authentication. The appellate court held that the printed post should have been admitted based upon the circumstantial evidence. *Kinda v. Carpenter*, 238 Cal.App.4th 989 regardless of whether that party is represented by counsel.