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

ELECTRONIC EVIDENCE AT MATRIMONIAL & FAMILY COURT HEARINGS & TRIALS

Introducing Text Messages, Social Media, Electronic Evidence & Videos into Evidence (Part 2)

FACULTY

Hon. Darlene Jorif Mangane (Part 1)
Support Magistrate

****Harry Tilis, Esq. (Part 2)****
Law Clerk to Hon. Paul Hensley

Program Coordinators: Hon. John J. Leo, Hon. Caren Loguercio, Hon. Catherine E. Miller, Hon. Darlene Jorif Mangane

December 8, 2022
Suffolk County Bar Association, New York

Like us on:

"The opinions, beliefs and viewpoints expressed herein are those of the authors and do not necessarily reflect the official policy, position or opinion of the Suffolk County Bar Association, Suffolk Academy of Law, their i Board of Directors or any of their members"

There's a whole new way to obtain your CLE certificate! It's fast, easy and best of all you can see the history of courses that you've attended!

Within 10 days of the course you attended, your CLE Certificate will be ready to view or print. Follow the instructions below:

1. Go to SCBA.org
2. Member Log In (upper right corner)
3. If you **do not** know your username or password, click the area below and enter your email that is on file with SCBA. Follow the prompts to reset your username and password.
4. After you log in, hover over your name and you will see "Quick Links". Below that you will see:
   a. My SCBA
   b. My CLE History
   c. Update My Information
   d. Update My Committees
5. Click on **My CLE History**, you will see the courses you have attended. Off to the right side you will see the Icon for certificates. You are now able to download the certificate, print it or save it. You may go to your history and review the courses you have taken in any given year!
6. **CLE certificates will no longer be mailed or emailed**. Certificates will be available within 10 days after the course.

HARRY TILIS, ESQ.

Harry is the law clerk to the Honorable Paul Hensley, County Court Judge and Acting Family Court Judge. Harry is also a past Dean of the Suffolk Academy of Law. A 1989 ***magna cum laude*** graduate of the Cornell Law School, Mr. Tilis lectures extensively for the Academy and other CLE providers on topics related to trial practices and developing trends in case law. He began his career in the corporate department of Proskauer, Rose, Goetz and Mendelsohn and has served as general counsel for industry leading companies before transitioning his practice to representation of small businesses, their entrepreneurs and their families. He is the author of The Art of Influence Simplified for Lawyers.

In addition to volunteering over 100 hours per year for the Empire Mock Trial Association and the American Mock Trial Association, Harry actively supports the American Foundation for Suicide Prevention. His work responsibilities include serving as one of the Counsel at First Appearance Attorneys in Suffolk County District Court.

Part 11

ELECTRONIC EVIDENCE & SOCIAL MEDIA

October 13, 2022

Stephen Gassman, Esq.
GASSMAN BAIAMONTE GRUNER, P.C.

Contents

ELECTRONIC EVIDENCE & SOCIAL MEDIA

Stephen Gassman, Esq.
GASSMAN BAIAMONTE BETTS, P.C.

I. COURT RULES & REQUIREMENTS

A. Section 202.12(b) of the Uniform Rules as well as Rule 1(b) of section 202.70(g). 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.

B. NYCRR § 202.12 (c)(3). Preliminary Conference

1. Where the court deems appropriate, establishment of the method and scope of any electronic discovery, including but not limited to (a) retention of electronic data and implementation of a data preservation plan, (b) scope of electronic data review, (c) identification of relevant data, (d) identification and redaction of privileged electronic data,(e) the scope, extent and form of production, (f) anticipated cost of data recovery and proposed initial allocation of such cost, (g) disclosure of the programs and manner in which the data is maintained, (h) identification of computer system(s) utilized, and (i) identification of the individual(s) responsible for data preservation;

C. Mandatory CLE - Cybersecurity

1. Effective January 1, 2023, 22 NYCRR Part 1500 amended to create a new mandatory CLE category of "Cybersecurity, Privacy and Data Protection, to require newly admitted and experienced attorneys to complete 1 credit hour in this category within 2 years of admission and during each biennial reporting cycle, respectively.

D. 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,...*"

E. 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".

F. 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.

G. 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.

H. 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]

II. SERVICE BY E-MAIL

A. *Synder v. Alternate Energy Inc.,* 19 M3d 954, 857 NYS2d 442 (Civ. Ct., NY Co., 2008) - 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.

B. In a proceeding seeking to terminate the parental rights of the father, the county sufficiently demonstrated that it was impractical for personal service of process to be effectuated pursuant to CPLR 308(5), as the father was deported from the United States to Jordan prior to the child being removed from the mother's care, the caseworker had multiple communications with the father through e-mail and none of the transmissions were returned as undeliverable, the father acknowledged receipt of information via e-mail during the pendency of the neglect proceeding and made requests for additional documentation from the caseworker, and the father never provided the caseworker with a physical address nor any other reasonable means of communication besides the e-mail address. *Matter of J.T.,* 53 Misc 3d 888 [Fam Ct 2016])

C. As prior attempts at ordinary service having proved impracticable, service of process on the respondent father via his email address is reasonably calculated to apprise the respondent of the instant proceeding; and it is ordered, that service of process via electronic mail at the respondent's most recent email address on or before May 18, 2013 is deemed acceptable. *Matter of N.Z. v A.G.*, 40 Misc 3d 696 [Fam Ct 2013])

III. DISCOVERY

A. The courts have further held that there is a two-pronged analysis for determining whether social media accounts are discoverable. First, the court determines whether the content in the accounts is material and necessary, and then it balances whether the production of this content would result in a violation of the account holder's privacy rights." *Fawcett v. Altieri,* 38 M3d 1022 (Supreme Court, Richmond Co., 2013)

B. Material and Necessary

[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

1. Social media account is material and necessary where the information "contradicts or conflicts with plaintiffs allege restrictions, disabilities, and losses, and other claims). *Patterson V. Turner construction Co.*, 88 A.D.3d 617 (1st Dept. 2011)

C. Relevance

1. To establish a factual credit for the discovery of a private or closed social media account by court order, a party must show credible facts that the adversary subscriber has posted information or photographs that are relevant. Additionally, the discovery request should be narrowly tailored seeking only social media relating to the claimed injuries arising from the accident. *Jennings v. TD Bank*, 2013 NY Slip Op 32783(U) (Supreme Court, Nassau Co, Brown, J.)

2. Digital fishing expeditions are no less objectionable than their analog antecedents. *Winchell V. Lopiccolo*, 38 M3d 458 (Supreme Court, Orange Co., 2012, Marx, J.)

IV. 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. The husband's request for production of the wife's personal computer and any other computers that she regularly used in the marital home was denied because the husband did not prove that what he sought was material and necessary and that it could not be procured in a less invasive and violative manner. This was especially the case because the information he sought was either protected by the attorney-client privilege or had already been admitted by the wife. *R.C. v. B.W.*, NYLJ, 04/03/08, p. 26, col. 1, S.Ct., Kings Co., Adams, J.

d. 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)

e. 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.

f. 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).)

V. 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)

VI. 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

1. 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.

VII. 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]

VIII. 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.

IX. 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)

X. 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."

XI. 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)

XII. 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.

XIII. 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.

XIV. EVIDENTIARY HURDLE - AUTHENTICATION - GENERALLY

1. Most significant issue for ESI - E-mails, text messages and social media data are subject to the same requirements for sentences he as traditional paper documents.
2. Non-testimonial evidence- writings, photographs, recordings – must be authenticated, i.e, the evidence is what it is purported to be. (FRE 901(a))
3. FRE 901(b) identifies ten nonexclusive examples of how authentication can be accomplished.
4. 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)
5. 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.

XV. CIRCUMSTANTIAL EVIDENCE AS BASIS FOR AUTHENTICATION

A. Cases

1. Proper to admit into evidence a series of text messages exchanged between a person purporting to be defendant's mother and the victim two days after the crime. There was sufficient authentication, because an extensive chain of circumstantial evidence left no doubt that the texts came from defendant. Among other things, these intimidating texts, which contained damaging admissions, reached the victim at a disguised phone number that she had shared with defendant shortly after the crime, but had not shared with anyone else. The texts revealed a detailed knowledge of the incident and the relationship between defendant and the victim, and they explicitly discussed the sexual encounter. The sender admitted having the victim's car, bag and phone, which were taken during the incident, and defendant was apprehended a day later driving the victim's car. Viewed as a whole, and not as individual fragments, the circumstantial evidence made it highly improbable that anyone other than defendant (including the unapprehended second participant in the crime) sent the texts. In addition, the sender's phone number was registered to a former female friend of defendant. *People v Washington*, 179 AD3d 522, 523 [1st Dept 2020])

2. 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)

3. 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"),

4. *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.

B. IM Communications – Circumstantial Evidence to Authenticate

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])

2. People v Clevenstine, 68 AD3d 1448, 891 NYS2d 511 [3d Dept. 2009] lv to appeal denied, 14 NY3d 799 [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).

3. 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]; **2 *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]). 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, 988 NE2d 529 (2013)

C. *Cf. Peo. v. Givans*, 45 AD3d 1460 (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.

XVI. 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." (Lorraine v. Markel Am. Ins., 241 F.R.D. 534, 555-56 [D. Md., 2007])

B. *Robmom v. Weberman,* 2002 WL 1461890 (S.Ct., Kings Co., 2002, Jones, J.) - 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.

XVII. AUTHENTICATION – EMAILS

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

B. 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."

XVIII. AUTHENTICATION BY HEADER

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

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

XIX. AUTHENTICATION BY E-MAIL THREAD

A. Authentication can also be established via an e-mail thread. For example, if 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, 2012.
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

XX. 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.

XXI. AUTHENTICATION BY DISCOVERY PRODUCTION

A. CPLR Rule 4540-a. Presumption of authenticity based on a party's production of material authored or otherwise created by the party. 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.

B. 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 F.Supp.2d 462 [S.D.N.Y. 2000])

C. Tip - reason to inventory all documents received during discovery. Specifically, Bates stamp everything received and send a confirmatory letter of what was produced if the producing party did not provide a detailed inventory of the records.

XXII. AUTHENTICATION BY TESTIMONY OF SENDER

STEPS

The electronic address placed on the e-mail is that of the claimed recipient.
The purpose of the communication (why it was sent)
If applicable, establish that the sender receives an earlier e-mail and replied to the earlier e-mail.
Establish that the e-mail was actually sent.
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. Larrythe 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.

XXIII. 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.

XXIV. 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.

XXV. 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.

XXVI. AUTHENTICATION - TEXT MESSAGES & IM'S

A. A document created by the complainant reflecting a series of text messages between the complainant and the defendant was admissible where the complainant's testified that the text messages were accurately and fairly reproduced. People v Enoksen, 175 AD3d 624 [2d Dept 2019])

XXVII. AUTHENTICATION BY TESTIMONY OF SENDER

STEPS

(1) The context of a message – why was 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.

XXVIII. 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 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 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?
A: Yes.
Q: Did you alter or modify in any way the text messages that appear on the transcript?
A: No.

XXIX. 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, 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 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. Foundations

1. Assuming the proponent is not the person was website posting is at issue, if foundation can be laid by simply having a witness testify that he or she is the person who

printed out the posting, that he or she recalls the appearance of the printout that he or she made from the social media site, and that he or she recognized the exhibit as that print out.

2. Assuming such a witness as above is not available, the proponent to have a witness testified 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 any members 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 unavailable, other relevant factors include to attribute the printout has adopted the user name shown on the profile page

6.Whether the person has shared his or hers social media password with other people

7. Whether there is a photograph on the persons or identities profile page that identifies a person to whom the proponent wishes to attribute the posting

8. Whether there is personal information of 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 friends?
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.

XXX. MATERIAL AND NECESSARY V. PRIVACY RIGHTS

A. *Romano v. Steelcase, Inc.*, 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. "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 joined in of life, all of which are material and relevant to the offense 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 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."

Defendant granted access to all Facebook and MySpace pages, including all deleted pages and related information as there was indication that the social networking sites contain information and consistent with her personal injury claims. Information was material and necessary to the defense and/or could lead to admissible evidence. "Defendant's need for access to the information outweighs any privacy concerns that may be voiced by the Plaintiff."

B. *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.

C. 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 non-party disclosure has been shown. The Husband claims that the *3 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 Misc. 3d 1013(A), 801 N.Y.S.2d 776 (S.Ct., Nassau Co., 2005, Balkin, J.)

D. *Griffin v. Maryland*, 19 A.3d. 415 (Md. 2011) - In a murder trial, the prosecution's attempt to introduce printouts from a MySpace page, to impeach a defense witness, was unsuccessful 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 punitive author could have accessed the computer and failed to acknowledge the possibility of a likelihood that another user could have created the profile in issue.

XXXI. AUTHENTICATION OF SOCIAL NETWORK PROFILE POSTINGS FROM A SOCIAL NETWORK SITE – SUGGESTED METHODS:

- Testimony from the purported creator of the social network profile and related postings;
- Testimony from persons who received the messages;
- Testimony about the contextual clues and distinctive aspects in the messages themselves tending to reveal the identity of the sender;
- Testimony regarding the account holders exclusive access to the originating computer and social media accounts;
- Expert testimony concerning the results of the search of the social media account holders computer hard drive;
- 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
- Expert testimony regarding how social network accounts are accessed and what methods are used to prevent unauthorized access.
- Testimony from persons who received the messages;
- Testimony about the contextual clues and distinctive aspects in the messages themselves tending to reveal the identity of the sender;
- Testimony regarding the account holders exclusive access to the originating computer and social media accounts;
- Expert testimony concerning the results of the search of the social media account holders computer hard drive;
- 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
- Expert testimony regarding how social network accounts are accessed and what methods are used to prevent unauthorized access.
-

XXXII. 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 Mardh 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)

XXXIII. OFFICIAL GOVERNMENT WEBSITES

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

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

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

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]; Secretary of State for "entity information" regarding corporate officers (*Munaron v. Munaron*, 21 Misc.3d 295, 862 N.Y.S.2d 796 [Sup. Ct. Westchester Co. 2008][Jamieson, J.

"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 A.D.2d 666, 537 N.Y.S.2d 177 (2d Dept.1989)*; Chasalow v. Board of Assessors of County of Nassau, 176 A.D.2d 800, 575 N.Y.S.2d 129 (2d Dept.1991). The Court informed the parties that it would be taking judicial notice of this fact at a Court conference."

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

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

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

Department of State (NYS) online search results for whether physician was licensed to practice medicine in NYS (;*F2;F2Proscan 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 .... 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."

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."

B. Private or commercial websites

1. Hospital website for asthmatic conditions and causes (*Gallegos v. Elite Model Management Corp.*, 758 N.Y.S.2d 777 [Sup. Ct. NY 2003])

2. 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 F.3d 1218, 1225 [10th Cir. 2007])

3. Mapquest for mileage distance (*In Re Extradition of Gonzales*, 52 F.Supp.2d 725, 731, n. 12 [Wd La. 1999])

XXXIV. 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]").

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

XXXV. SELF-AUTHENTICATION (RULE 902)

A. Rule 907(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 "contain'3d] the internet domain address form 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])

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

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

F. 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.*

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

XXXVI. PHOTOGRAPHS

A. *People v. Lenihan*, 30 M3d 289 (S.Ct., NY Co., 2010) - Defendant precluded from confronting witnesses with printouts of MySpace photos depicting him and gang clothing because of the easy ability to digitally or at its photographs on the computer. Accordingly, proof that a message of 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. *Peo. V. Jordan*, 181 A.D.3d 1248 (4th Dept. 2020) - Certain Facebook images of defendant and other people were properly authenticated by the testimony of a witness who had personal knowledge of the people in the images at a verified that the images accurately represented the subject matter depicted.

XXXVII. EVIDENTIARY HURDLE – HEARSAY

1. Preliminary Considerations

a. Statement

b. Human Declarant

c. Admitted for truth?

(1) Email between co-workers, when offered to prove only that relationship existed between them, not to prove the truth of the email's contents. (*Siddiqui*, 235 F.3d 1318)

(2) Exhibit showing defendant's web site content on a particular day, when offered not for the truth of its contents, but to show trademark and copyright infringement. *Perfect 10, Inc., 213 F.Supp.2d 1146*

d. Fit within recognized exceptions

2. **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. Example- supermarket – box of cereal – checkout counter – scanned – credit card put in machine – output of a receipt – assume receipt is relevant to issue in case – not hearsay - transaction devoid of a human declarant
    4. 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.

3. **Hearsay Exception - Admission of Party-Opponent**

    1. any statement which is against the interest of the party at the time of trial (or might not have been against the interest of the party at the time it was made)
    2. 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]

4. **Hearsay Exception - State of Mind**

    1. 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])

5. **Hearsay Exception - Business Record Rule (CPLR 4518)**

    1. *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 admissible under the business records exception.
    2. Computer printouts - 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); 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 A.D.2d 985, 692 N.Y.S.2d 563 (4th Dep't); *In re Thomma*, 1996, 232 A.D.2d 422, 648 N.Y.S.2d 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 N.Y.S.2d 367, 374, 315 N.E.2d 441, 446; *Sager Spuck Statewide Supply Co., Inc. v. Meyer*, 298 AD2d 794, 751 NYS2d 318 (3d Dept. 2002) (computer printouts summarizing equipment suppliers declining gross sales and profits admissible for the limited purpose of aiding jury in comprehending voluminous data already in evidence)

3. *Monarch Fed. Sav. & Loan Assn. v. Genser*, 156 N.J. Super, 107 (1977) -- Business record rule exception applied where the evidence that the electronic computing equipment at issue was recognized as standard; that the entries were made in the regular course of a regular conducted business activity at or reasonably near the happening of the event recorded by or from someone within the business possessing personal knowledge that the computer process produces an accurate result when correctly employed and properly operated; and that the computer process was so employed and operated with respect to the matter at hand.

6. **Hearsay Exception - Prior Inconsistent Statement**

1. In a termination of parental rights case, the court considered the father statement on his MySpace profile that he did not want children. (*In re T.T., 228 S.W.3d 312, 322-23 (Tex. Ct. App. 2007)*
2. CPLR 4514 – impeach any witness with prior inconsistent statement if in writing subscribed by the witness or under oath
3. Argument - If email satisfies "writing requirement" for statute of frauds, should for purposes of impeachment via CPLR 4514 – prior inconsistent statement
4. Prior Inconsistent Statement – when defense counsel questioned defendant's ex-girlfriend about her conversations with the complainant via text message and social media, although the testimony was hearsay, it was admissible as evidence of a prior inconsistent statement (an exception to the hearsay rule). Peo. v. Morales, 160 A.D.3d 1414 (4th Dept. 2018)

7. **Hearsay Exception - New York's common law public records exception**

1. *Miriam Osborn Memorial Home Assn., v. Assessor of the City of Rye*, 9 Misc.3d 1019, 800 N.Y.S.2d 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 A.D.2d 943, 655 N.Y.S.2d 219 (4th Dept.1997)

8. **CPRL 4539 – Best Evidence**

    1. If any business, institution, or member of a professional calling, in the regular course of business or activity has made, or recorded any writing, entry, print or representation and in the regular course of business has recorded, copied or reproduced it by any process, including reproduction, which accurately reproduces or forms a durable medium for reproducing the original, such reproduction, when satisfactorily identified, is as admissible in evidence as the original, whether the original is in existence or not, and an enlargement or facsimile of such reproduction is admissible in evidence if the original reproduction is in existence and available for inspection under the direction of the court. The introduction of a reproduction does not preclude admission of the original
    2. A reproduction created by any process which stores an image of any writing, entry, print or reproduction and which does not permit additions, deletions or changes without leaving a record of such additions, deletions, or changes, when authenticated by competent testimony or affidavit which shall include the manner or method by which tampering or degradation of the reproduction is prevented, shall be as admissible in evidence as the original.

XXXVIII. HEARSAY; POLICE REPORT; ADMISSION

A. Absent a proper foundation, a party's admission contained in an uncertified police accident report is inadmissible. The use of a statement recorded in a police accident report involves two levels of hearsay, each of which is required for admissibility. First, the report itself must be admissible. A properly certified police accident report (CPLR 4518[c]) is admissible where the report is based upon the officer's personal observation and while carrying out police duties. Second, the statement recorded must satisfy a hearsay exception. Although a party's admission is an exception to the hearsay rule, the admission cannot be received in evidence where the business record containing the purported admission is not itself in admissible form. *Yassin v. Blackman,* 188 AD3d 62, 131 NYS3d 53 (2d Dept. 2020)

XXXIX. EVIDENTIARY HURDLE - PREJUDICE

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

XL. ISSUE OF EXPECTATION OF PRIVACY

A. *E-Docs Stored at Work*

1. *Scott v. Beth Israel Med. Ctr.*, 17 Misc.3d 934, 847 N.Y.S.2d 436 [Sup. Ct. N.Y Co. 2007][Ramos, J.] 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.

2. *Curto v. Medical World Communications Inc.*, 2006 WL 1318387 (EDNY, 5/16/06) – 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.

3. *U.S. v. Finazzo*, 2008 U.S. Dist. LEXIS 30604 (S.D.N.Y. 3/27/08) – In determining whether there has been a waiver of the attorney-client privilege when office computer used to communicate with attorney, the 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.

XLI. CELL PHONE TRACKING

A. 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.

B. *People v. Moorer*, NYLJ, 2/22/13 (County Ct., Monroe Co., DeMarco, J.) -- 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 devices powered up, "a person necessarily has no reasonable expectation of privacy with respect to the phone's location." While cell phone uses 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.

C. Garcia v. City of Laredo, No. 11-41118 (U.S.C.A., 5th Cir., 2012) - 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".

D. Miller v. Lewis, NYLJ, 4/25/13 (S.Ct., Kings Co., Ruchelsman, J.) -- 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.

XLII. GPS DEVICES

A. Civil Case

1. *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])

B. Criminal Case

1. *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.

XLIII. CLIENT READING SPOUSE'S EMAILS

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) - an attorney must take "reasonable remedial measures, including, if necessary, disclosure to the tribunal unquote if the attorney becomes aware of the client thereof the person intends to engage in criminal or forcefully conduct in relation to the proceeding.

XLIV. 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 orsimilar purposes. In advising a client, attorneys should be mindefendantul of their ethical responsibilities udner 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 reveal produce..l.[nor] (3) conceal or knowlingly fial 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 ot 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."

XLV. IMPROPERLY OBTAINED DISCOVERY

A. Recusal

1. *Matter of Beiny*, 129 AD2d 126, 517 NYS2d 474 (1st Dept. 1987) - 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

XLVI. 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 was 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.

XLVII. LITIGATION HOLDS FOR ESI; SPOILATION

A. Spoliation occurs when a party intentionally destroys evidence or negligently destroys evidence that the party has a duty to preserve (*Weiss v. Industrial Enterprises, LTD*, 7 AD3d 518).

B. Proof of Spoliation (*Victor Stanley v. Creative Pipe Inc.*, 2008 WL 2221841 (D. Md. May 2009, 2008); See, *Zoom HD Holdings v. EchoStar Satellite LLC*, 93 AD3d 33, 939 NYS2d 321 (1st Dept. 2012)

- that the party having control over the evidence had an obligation to preserve it when it was destroyed or altered;
- that the destruction or loss of the evidence was accompanied by a culpable state of mind; and
- that the evidence that was destroyed or altered was relevant to the claims or defenses of the party seeking discovery.

C. When Does Duty to Preserve Arise

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.)

D. 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.*

E. 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)

b. *Chen v. Fischer*, 73 AD3d 1167, 901 NYS2d 682 – Prior to final judgment of divorce, wife sued husband for personal injuries for alleged physical and emotional abuse during the marriage. Due to wife deleting from her computer's hard drive materials that she had been directed to produce in the personal injury action, court directed dismissal of her complaint in its entirety.

c. Spoliation occurred requiring dismissal of plaintiff's action where between date that defendant demanded inspection of plaintiff's computer, and date of inspection, plaintiff deleted files, images and folders and installed software program designed to permanently remove data from the computer's hard drive. *Ingoglia v. Barnes and Noble College Booksellers Inc.*, 48 AD3d 636, 852 NSY2d 337 (2d Dept. 2008)

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)

F. 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)

G. 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.)

2. A proper sanction in a matrimonial litigation where plaintiff installed spyware on the other party's phone, invoked the Fifth Amendment protections on the issue, and intentionally destroyed evidence as to what the spyware actually intercepted, was to infer that the plaintiff violated the defendant's attorney-client privilege, and that plaintiff's causes of action in the complaint relating to the financial issues of the case other than child support should be stricken. A party that seeks sanctions for spoliation of evidence must show that the party having control over the evidence possessed an obligation to preserve it at the time of its destruction, that the evidence was destroyed with a 'culpable state of mind,' and 'that 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. Where the evidence is determined to have been intentionally or wilfully destroyed, the relevancy of the destroyed documents is presumed. Where plaintiff violated the defendant's attorney-client privilege, the preclusion of documents is

not an appropriate alternative sanction because the plaintiff will always be privy to any litigation strategy of the defendant that he gained through secretly intercepting her privileged communications. ***C. C. v. A. R.***, 192 A.D.3d 654, 143 N.Y.S.3d 404 (2d Dept. 2021)

H. No Sanction – *O'Loughlin v. Sweetland*, 98 AD3d 983, 951 NYS2d 160 (2d Dept. 2012) – Affirmed refusal to impose any type of sanction upon a forensic custody evaluator who destroyed audiotapes of interviews she conducted in the course of her evaluation, the court commenting that "The Family Court properly denied the mother's motion to preclude the introduction into evidence of the report and testimony of a forensic evaluator, or, alternatively, for a negative inference to be drawn concerning the evaluator's credibility, based upon the evaluator's destruction of certain audiotapes of interviews she conducted in the course of her evaluation. The record does not support the mother's contention that the missing audiotapes denied her the ability to effectively cross-examine the forensic evaluator (*see generally Kesseler v Kesseler*, 10 NY2d 445 [1962])."

I. Finding of Gross Negligence

a. The Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC, 2010 WL 184312 (S.D.N.Y. 2010), Scheindlin, J.- types of failures:

- the failure to issue a written litigation hold;
- the failure to identify key players and to ensure that their electronic and paper records are preserved;
- the failure to cease the deletion of e-mail or to preserve the records of former employees that are in a party's possession, custody or control; and

the failure to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.

- Caveat - Under some circumstances, placing 'total reliance on [an] employee to search and select what that employee believed to be responsive records without supervision from Counsel', can amount to gross negligence. Judge Scheindlin noted that 'not every employee will require hands-on supervision from an attorney. However, attorney oversight of the process, including the ability to review, sample, or spot-check the collection efforts is important. The adequacy of each search must be evaluated on a case by case basis."

XLVIII. PRIVILEGE LOG

A. Applies not only to direct communications between an attorney and client, but also to the Work Product Doctrine (CPLR 3101(c)) and Material Prepared for Litigation (CPLR 3103 (d))

B. *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 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.

APPENDICES

N.Y.Ct.Rules, § 202.12

§ 202.12. Preliminary Conference

(c) The matters to be considered at the preliminary conference shall include:...

(2) establishment of a timetable for the completion of all disclosure proceedings, provided that all such procedures must be completed within the timeframes set forth in subdivision (b), unless otherwise shortened or extended by the court depending upon the circumstances of the case;

(3) Where the court deems appropriate, establishment of the method and scope of any electronic discovery, including but not limited to (a) retention of electronic data and implementation of a data preservation plan, (b) scope of electronic data review, (c) identification of relevant data, (d) identification and redaction of privileged electronic data,(e) the scope, extent and form of production, (f) anticipated cost of data recovery and proposed initial allocation of such cost, (g) disclosure of the programs and manner in which the data is maintained, (h) identification of computer system(s) utilized, and (i) identification of the individual(s) responsible for data preservation;

NY Ct R § 202.12

(k) The provisions of this section shall apply to preliminary conferences required in matrimonial actions ...only to the extent that these provisions are not inconsistent with the provisions of sections 202.16, 202.56 and 202.60 of this Part, respectively.

Sample Litigation Preservation Letter

Re: Smith v. Smith

Dear _____:

Plaintiffs Demand That Defendant[1]F[2] *Preserve All Documents, Tangible Things and Electronically Stored Information Potentially Relevant to the Issues in the Above-Entitled Action. You Should Anticipate That Much of the Information Subject to Disclosure or Responsive to Discovery in This*

[2] As used in this document, references to "Defendant", "You" and "Your" refers to the defendant and his officers, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

Matter Is Stored on Your Current and Former Computer Systems and Other Media and Devices (Including Personal Digital Assistance, Voice Messaging Systems, Online Repositories and Cellphones).

Electronically Stored Information (Hereinafter "ESI") Should Be Afforded the Broadest Possible Definition and Includes, but Is Not Limited to, Potentially Relevant Information Electronically, Magnetically or Optically Stored Such As Digital Communications (e.g., E-Mail, Voice Mail, Instant Messaging); Word Processing Documents, Spreadsheets and Tables; Accounting Application Data (e.g., Quick Books, Microsoft Money, Peachtree Data Files), Image and Facsimile Files, Sound Recordings (e.g., WAV. and. MP3 files), databases, calendar and diary application data, network access and server activity logs, Back Up and Archival files.

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably assessible to you but also in areas you may deem not reasonably assessible. You are obliged to preserve potentially relevant evidence from both these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both assessible and inassessible ESI is reasonable and necessary. You must also identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably assessible. For good cause shown, the court may then order production of the ESI, even if it finds that it is not reasonably assessible. Accordingly, even ESI that you deem reasonably inassessible must be preserved in the interim so as not to deprive the plaintiff of his/her right to secure the evidence or the court of its right to adjudicate the issues.

You must act immediately to preserve potentially relevant ESI. Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Please be advised that sources of ESI are altered and erased by continued use of defendant's computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently or responsibly to prevent loss or corruption of ESI.

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI.

You should anticipate that the employees, officers or others employed by the defendant may seek to hide, destroy or alter ESI and you should act to prevent or guard against such actions.

Especially where company machines have been used for Internet access or personal communications, you should anticipate that users may seek to destroy or delete information they regard as personal, confidential or embarrassing and, in doing so, may also delete or destroyed potentially relevant ESI. This concern is not unique to defendant or his employees and offices. It is simply an event that regularly occurs in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information effectively in the litigation.

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it.

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems may contain potentially relevant ESI. If so, the same requirements that have been outlined above should be applicable to such home systems, laptops, and any other ESI venues.

As hard copies do not preserve electronic search ability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that are subject to your direction or control. Accordingly the defendant should notify any current or former employees, custodians or others in possession of potentially relevant ESI to preserve same to the full extent of defendant's obligation to do so, and take reasonable steps to secure such compliance.

I am available to discuss reasonable preservation steps and an acceptable protocol for forensically sound preservation. However, you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay.

Very truly yours,