ADMISSIBILITY OF ELECTRONIC/DIGITAL EVIDENCE: EVIDENTIARY HURDLES AND RELATED ISSUES

By:

Michael J. Hutter, Esq.

Professor of Law
Albany Law School
80 New Scotland Avenue
Albany, NY 12208
(518) 445-2360
mhutt@albanylaw.edu

Special Counsel
Powers & Santola, LLP
39 North Pearl Street
Albany, NY 12207
(518) 465-5995
mhutter@powers-santola.com

April 2, 2019

TABLE OF CONTENTS

PART THREE
APPLICATION OF EVIDENTIARY RULES
TO ELECTRONIC EVIDENCE

PART FOUR
JUDICIAL NOTICE

PART FIVE
ETHICS AND PRIVILEGE ISSUES

PART ONE

INTRODUCTION

I. ELECTRONIC EVIDENCE – A FACT OF LIFE

A. Generally

1. As aptly stated:

"It has become cliché to observe that electronic evidence has changed every aspect of modern trial practice. From smartphones, to email, to Facebook, we each leave an electronic trail of our daily lives scattered across servers, hard drives, and the cloud. No wonder litigants and their lawyers have come to rely on that data to prove or refute the crucial elements of their cases. In criminal cases, it might be GPS locations bouncing off repeaters near the crime scene. In a divorce, it might be that flurry of late-night text messages. In trade secret litigation, look for those megabytes of data that the employee downloaded right before quitting. Whatever the case, the proof of the trial is now more likely to be digital than tangible." (Aveni, "New Federal Evidence Rules Reflect Modern World," 43 Litigation News [ABA], Spring 2018, at p.11).

2. And:

"Unless one handwrites information on a piece of paper, and thereafter shreds, burns or otherwise discards the paper without it coming near a computer, scanner or smartphone camera, almost nothing in our world exists without some analog in electronic storage. Such is our ever-evolving, ever-more-technological world .... Consequently, that electronically stored information and documentation, once it is disclosed through the discovery process, and evaluated by attorneys and their experts, then becomes the subject of that next hurdle in litigation – the proffer of evidence at trial." (Fox, "I Show You Exhibit E for Identification," 22 NYSBA Litigator [NYSBA], Spring 2017, at p.14).

B. Value

1. Electronic/digital evidence is a veritable cache of relevant evidence that can be dispositive, or at the very least helpful, in proving one's case or defeating the adversary's case. This is especially true with respect to

social media. As one commentator has observed: "If a picture is worth a thousand words, a person's social media [page] is priceless to a trial lawyer. With just a few clicks, a trial lawyer can obtain raw unfiltered evidence of a [party's] activities, relationships, emotions and thoughts." (Morales, "Social Media Evidence," 60 The Advocate (Texas) 32 [Fall 2012]).

II. ADMISSIBILITY OF ELECTRONIC/DIGITAL EVIDENCE

A. Evolving Attitudes

1. "Anyone can put anything on the Internet . . . [H]ackers can adulterate the content on *any* website from *any* location at *any* time . . . [E]vidence procured off the Internet is adequate for almost nothing." (*St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F.Supp.2d 773, 775 [S.D. Tex. 1999]). It is in the eyes of some "voodoo information." (*Id.*). On the other hand, some courts have applied a more lenient standard. (*See, Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146 [CD Cal.2002] [a "reduced evidentiary standard" applied to the authentication of exhibits purporting to depict the defendant's website postings during a preliminary injunction motion. The court found that the exhibits had been authenticated because of circumstantial indicia of authenticity, a failure of the defendant to deny their authenticity, and the fact that the exhibits had been produced in discovery by the defendant. The court declined to require proof that the postings had been done by the defendant or with its authority, or evidence to disprove the possibility that the contents had been altered by third parties].)

2. Since 1999, judicial attitudes have for the most part changed. While overcoming initial reluctance to admitting ESI, "'courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources.'" (*People v. Johnson*, 51 N.Y.S.3d 450 [Co Ct. Sullivan Co. 2015] [Labuda, J.], quoting *Lorraine v. Market American Ins. Co.*, 241 F.R.D. 534, 543 [D. Md. 2007]). But "[s]ome courts have suggested applying 'greater scrutiny' or particularized methods for the authentication of evidence derived from the Internet due to a 'heightened possibility for manipulation.' . . . [W]e are skeptical that such scrutiny is required . . . ." (*United States v. Vayner*, 769 F.3d 125, 131, n. 5 [2d Cir. 2014]).

3. Commentators have sought to impose at least a higher authentication bar based on forgery concerns unique to social media evidence. (*See, e.g.*, Miller and White, "The Social Medium: Why The Authentication bar Should Be Raised For Social Media Evidence," 87 Temple Law Review Online 1 [2014]).

B. Role of Rules of Evidence

1. The New York's law of evidence, the Federal Rules of Evidence and state statutory evidence codifications based on the Federal Rules of Evidence, and common law evidence jurisdictions do not separately address the admissibility of electronic evidence. The courts apply the same rules of evidence as they do to other types of evidence to determine admissibility issues.

2. Thus, electronic evidence is treated no differently from other types of evidence, e.g., hard copy documents. Courts reject the view that electronic evidence has rendered basic common law evidence rules obsolete and requires a new set of evidence rules. (*See, In Re F.P.*, 878 A.2d 91, 95 [Pa. Super. Ct. 2005][rejecting plea to create "a whole new body of law" just to deal with ESI]).

3. However, specific rules are being adopted to cover recurring issues of admissibility of electronic evidence. (*See e.g.*, CPLR 4511 (c); FRE 902[13] and 902 [14]).

C. Application of the Rules

1. "[Admissibility] issues can be resolved by relatively straightforward application of existing principles in a fashion very similar to the way they are applied to . . . more traditional exhibits." (Joseph, Internet and Email Evidence [available at www.jha.com/us/articles).

2. In essence, electronic evidence is admissible whenever comparable oral testimony or hardcopy exhibit would be admissible.

3. Nonetheless, as stated by the Second Circuit, "attempting to apply established [evidence] law in the fast-developing world of the Internet is somewhat like trying to board a moving bus." (*Bensusan Restaurant Corp. v. King*, 126 F.3d 25, 27 [2d Cir. 1997]). Thoughtfulness is required.

4. For an informative discussion, see *The Philip D. Reed Lecture Series Advisory Committee On Evidence Rules: Panel Discussion: Symposium On The Challenges Of Electronic Evidence*, 83 Fordham L. Rev. 1163 (2014).

III. APPLICATION ON SUMMARY JUDGMENT MOTIONS

A. Generally

1. As stated in *Lorraine v. Markel American Ins. Co.* (241 F.R.D. 534, 536 [D. Md. 2007]): "To be entitled to consideration on summary judgment, the evidence supporting the facts set forth by the parties must be such as would be admissible in evidence. See FRCP 56(c). With regard to documentary evidence, this Court previously has held that,"[u]nsworn, unauthenticated documents cannot be considered on a motion for summary judgment. To be admissible at the summary judgment stage, documents must be authenticated by and attached to an affidavit that meets the requirements of Rule 56(e) – that the documents be admissible in evidence."

PART TWO
BASIC EVIDENCE RULES

I. INTRODUCTION

A. Applicable Rules

1. Federal Magistrate Judge Paul W. Grimm made the following instructive observation:

"Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI *relevant* as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it *authentic* as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is

offered for its substantive truth, is it *hearsay* as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an *original* or *duplicate* under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of *unfair prejudice* or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance." (*Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 538 [D. Md. 2007]).

2. While other evidence rules may be applicable in *sui generis* situations, the rules mentioned by Judge Grimm are paramount.

B. Both Federal and State Evidence Rules

1. These evidence rules are in large part identical in all jurisdictions.

2. Of course, the attorney must check for variations in his/her state.

II. RELEVANCE

A. Generally

1. The overarching evidence rule governing ALL offered Evidence is the rule of relevancy – only relevant evidence is admissible.

2. New York law recognizes evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.

3. In applying this definition the issues will be whether the evidence is offered to prove a material fact and whether it is logically probative of that fact.

4. In view of the wide variety of electronic evidence and the increasing amount of information will post on social media sites or email, there is a lot of evidence that is potentially relevant in a given action.

B. Purpose

1. Substantive – prove a fact to establish elements of cause of action or defense. (*See e.g.*, *Johnson v. Ingalls*, 944 NYS2d 654 [App. Div 2012][In this auto accident case, the trial court after an *in camera* review excluded the majority of the photographs obtained from P's Facebook account that Ds proffered as unduly prejudicial, cumulative or insufficiently probative, but permitted use of approximately 20 photos during P's cross examination. P claimed that, as a result of her injury, she suffered severe anxiety, vertigo, constant migraines and pain for a period of about two years, that her anxiety prevented her from going out or socializing with friends, and that she required antidepressant medication. The photos admitted were taken over a 1½-year period beginning shortly after the accident. They depicted P attending parties, socializing and vacationing with friends, dancing, drinking beer in an inverted position referred to in testimony as a "keg stand," and otherwise appearing to be active, socially engaged and happy. They further revealed that P consumed alcohol during this period, contrary to medical advice and her reports to her physicians. Court held: "The photographs had probative value with regard to P's claimed injuries, their evidentiary prejudice, and we find no abuse of discretion in their admission."]; *Melody M. v. Stephen M.,* 962 NYS2d 364 [App. Div. 2013]
[Court affirmed Family Court's modification of custody order, noting, among other things, that the child's mother referred to the child as an "A**hole" on her Facebook page and further demeaned and insulted him on that page as well.]).

2. Impeachment – attack a witness's credibility. (*See e.g., State v. Jacobs, 2017 WL 3837212* [Kan. Ct. App.] [trial court also allowed the admission of photos from Jacobs' Facebook page which allegedly showed him smoking marijuana. This was allowed as impeachment testimony after Jacobs had claimed that he no longer was involved with marijuana after his prior conviction]; *People v. Webb,* 2014 WL 5306415 [Mich. App. Ct] [In this sex abuse prosecution, Court held "credibility of defendant's stepdaughter was reasonably called into question by a text message she sent to her uncle indicating that defendant hadn't touched her since she was a very young child, which contradicted her testimony that defendant had never behaved inappropriately towards her or required her to do inappropriate things with complainant. The trial court reasonably determined that the text messages were admissible to aid the jury in assessing defendant's

stepdaughter's credibility. The court did not err by admitting the text messages for this narrow purpose, and defendant has not presented any evidence that the messages were improperly used by the jury."]).

III. AUTHENTICATION

A. Rule

1. Offered evidence must satisfy FRE 901, or the state equivalent, which mandates that the evidence offered must be shown to be "authentic."

2. Authentication refers to the requirement that before a writing, document, tangible object or test result is admitted, there must be and evidentiary showing that the proffer is what the proponent claims it to be unless it falls within the limited category of items that are deemed self-authenticating. All jurisdictions follow the authentication rules as set forth in Article IX of the Federal Rules of Evidence. FRE 901(b) sets forth examples of authentication methods and FRE 902(a) sets forth categories of items that can be deemed self-authenticating.

B. Establishing Authentication

1. Authentication is established by the introduction of sufficient proof upon which a reasonable juror could find in favor of authentication. The determination is made by the trial court.

2. The methods identified by FRE 901(b), which are recognized in New York, are non-exclusive. (Advisory Committee's note ["The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law."). Thus, litigants may use any of the methods listed in the Rule, any combination of them, or any other proof that may be available to carry their burden of showing that the proffered exhibit is what they claim it to be.

(a) In 2018, the Legislature enacted two methods governing authentication, CPLR 4511 (c) which addresses authentication of digital mapping images, *e.g*, Google maps; and CPLR 4540-a which is applicable to documents produced pursuant to CPLR article 31 document demands.

3. As Judge Grimm notes: "This requirement of showing authenticity or identity falls into the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in FRE 104(b). . . . A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. This is not a particularly high barrier to overcome." It means only that "[t]he question for the court under FRE 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is....' The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* ultimately might do so." (*Lorraine*, 241 FRD at 542).

IV. HEARSAY

A. Rule

1. Hearsay is a *statement*, an oral or written assertion or non-verbal conduct intended as an assertion, made *by a person* other than while testifying at a trial which is offered to prove the truth of the matter asserted. (FRE 801[a]).

(a) Note a statement must be involved which must be assertive. The Federal Rules of Evidence do not define an "assertion." However, courts have held that "the term has the connotation of a positive declaration." (*See, e.g.*, *United States v. Lewis*, 902 F.2d 1176, 1179 [5th Cir. 1990)] *Lexington Ins. Co. v. W. Penn. Hosp.*, 423 F.3d 318, 330 [3d Cir. 2005]).

(b) The statement must be made by a person.

2. Hearsay is inadmissible unless there is an applicable exception or its admissibility is constitutionally compelled. The rule and its exceptions ae set forth in Article VIII of the federal Rules of Evidence.

3. In criminal cases, a hearsay statement admissible under a pertinent exception is still subject to exclusion under the rule set forth in *Crawford v. Washington* (541 US 36 [2014]) and its progeny.

B. Four Issues

1. Is the evidence a statement?
2. Was the statement made by a declarant-person?
3. Is the statement being offered to prove the truth of its contents?
4. If hearsay, is there an applicable exception?

V. BEST EVIDENCE

A. Rule

1. The best evidence rule requires that when a party seeks to prove the contents of a writing, photograph or recording, it must produce the original thereof or explain its absence before secondary evidence of its contents may be admitted. (FRE 1002; *see* 1003-1008). An original is defined by FRE 1001(3) as: "the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An original of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."

2. FRE 1003 provides in essence that duplicates are co-extensively admissible as originals, unless there is a genuine issue as to the authenticity of the original, or the circumstances indicate that it would be unfair to admit a duplicate in lieu of an original. A duplicate is defined by FRE 1001(4) as: "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original."

VI. UNFAIR PREJUDICE

A. Rule

1. Even where relevant evidence is admissible, a court may still exclude the evidence in the exercise of discretion if its probative value is substantially outweighed by the danger that it will unfairly prejudice the other side or mislead the jury. (FRE 403).

2. There is no reason why this rule does not apply to electronic evidence. (*Lorraine v. Markel American Ins. Co.*, 241 F.R.D. at 538; *Rice v. Reliastar Life Ins. Co.*, 2011 WL 11685520 [MD La.]).

B. Application to Electronic Evidence

1. Judge Grimm has made the following observation about FRE 403: "Although Rule 403 may be used in combination with any other rule of evidence to assess the admissibility of electronic evidence, courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in the following circumstances: (1) When the evidence would contain offensive or highly derogatory language that may provoke an emotional response. (2) When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation. (3) when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under FRE 1006, Weinstein at § 1006.08[3] ("Summary evidence is subject to the balancing test under Rule 403 that weighs the probative value of evidence against its prejudicial effect."); and (4) In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence. (St. Clair, supra [Court expressed extreme skepticism regarding the reliability and accuracy of information posted on the internet, referring to it variously as "voodoo information". Although the court did not specifically refer to Rule 403, the possibility of unfair prejudice associated with the admissibility of unreliable or inaccurate information, as well as for confusion of the jury, makes Rule 403 a likely candidate for exclusion of such evidence]". *(Lorraine, supra,* at 585*)*.

PART THREE
APPLICATION OF EVIDENTIARY RULES TO ELECTRONIC EVIDENCE

I. COMPUTER RECORDS

A. Generally

1. In determining the admissibility of a computer printout of information contained in computerized records, it is important to separate

them into two distinct categories: computer-generated records and pre-existing computer-stored. (*See, United States v. Khoroozian,* 333 F.3d 498, 506 [3d Cir. 2003]; *State v. Gojcaj,* 92 A.3d 1056, 1067-1068 [Conn. App. 2014] [discussing various states' practices with respect to the distinction]; *People v. Hawkins*, 121 Cal.Rptr.2d 627, 642-643 [2002][same]; *People v. Holowko*, 109 Ill.2d 187, 191-192, 486 N.E.2d 877, 878-879 [1985]; *see also,* DOJ Computer Crime and Intellectual Property Section [CCIPS], "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", Evidence – Chapter 5, pp. 191-197 [2009], available at https://www.justice.gov/criminal-ccips/ccips-documents-and-reports).

(a) Computer-stored records are documents or databases that contain the input of humans and "happen" to be in electronic form. While they are, in essence, the electronic equivalent of handwritten documents, they have been created or stored by electronic means from the outset and have never been maintained as a paper document. Examples are bookkeeping records; records of business transactions.

(b) Computer-generated records are records that are created by process that does not involve any human input other than human input that triggers these processes. Examples are telephone records; email header information; tome and date stamps; electronic banking records [ATM]; EZ-Pass date; and log-in records from an ISP.

B. Foundation: Hearsay

1. Hearsay is generally defined to encompass an oral or written assertion, and non-verbal assertion of a person. Accordingly, nothing said by a machine is hearsay. As noted in the CCIPS (p. 191): "Increasingly, courts have recognized that many computer records result from a process and are not statements of persons — they are thus not hearsay at all. *See, United States v. Washington,* 498 F.3d 225, 230-31 (4th Cir.2007) (printed result of computer-based test was not the statement of a person and thus would not be excluded as hearsay); *United States v. Hamilton,* 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated header information was not hearsay as "there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801"); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) ("nothing 'said' by a machine . . . is hearsay") (quoting 4 Mueller & Kirkpatrick, *Federal Evidence* § 380, at 65 (2d ed. 1994))."

2. Accordingly, the courts are in general agreement that computer generated records that do not contain statements of persons do not implicate the hearsay rule. (*See, e.g., People v. Stultz*, 726 N.Y.S.2d 437 [App. Div. 2001][caller ID]; *United States v. Washington,* 498 F.3d at 230-231 [raw data generated by lab machines from testing of a person's blood to determine presence of alcohol or drugs; *United States v. Hamilton*, 413 F.3d 1138 [10th Cir. 2005][computer-generated "header" information]; *Holowko, supra* [automated trap and trace records]; *United States v. Duncan*, 30 M.J. 1284 [1990][ATM transactions]; *Tatum v. Commonwealth*, 17 Va. App. 585, 440 S.E.2d 133 [1994][caller ID]; *State v. Dunn*, 7 S.W.3d 427 [Mo. 2000][long distance billing record]; *Murray v. State*, 804 SW2d 279 [Tex. App. 1991] [electronic lock device]).

(a) In *State v. Hall* (976 SW2d 121 [Tenn. 1998]), the Tennessee Supreme Court addressed the admissibility of printouts of telephone bills and held: "[C]omputer generated records are not hearsay: The role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.... In this case, the record reflects that persons with special knowledge about the operation of the computer system gave evidence about the accuracy and reliability of the computer tracing so as to justify the admission of the computer printouts. The rule against hearsay is not implicated.... Here, the state did not present the testimony of an AT&T records custodian, but there was testimony from ... [the records custodian for GTE telephone company in Texas]. He testified that AT&T's billing system is highly reliable and that all local phone companies doing business with AT&T have the exact same billing system.... [H]is testimony was sufficient to confirm the reliability of the telephone bill[.]".

(b) In *United States v. Lizarraga-Tirado* (789 F.3d 1107 [9th Cir. 2015]), the Ninth Circuit held admissible satellite image of region where defendant was arrested and tack and global positioning system (GPS) coordinates on satellite image of region where defendant was arrested were not hearsay, noting: (1) Google Earth images were not themselves hearsay as photographs are not hearsay, as they make no "assertion" but "merely depicts a scene as it existed at a particular time," and same is true of Google Earth images; (2) a "tack" on Google Earth image, produced by user "clicking any spot on the map," which generates coordinates, presents a

more difficult hearsay question as labeled markers added to a satellite image "do make clear assertions," like a dot labeled with the name of a town, or "the label 'Starbucks' next to a building," which "asserts that you'll be able to get a Frappuccino there" and if the tack were placed "manually" on a Google Earth image and then labeled with coordinates, it would be "classic hearsay"; (3) but court here takes judicial notice that tack is "automatically generated by the Google Earth program, so it is not hearsay as "the relevant assertion isn't made by a person," but "by the Google Earth program" and the real work is done by the program; and (4) the proponent must "show that a machine is reliable and correctly calibrated, and that the data put into the machine (here, the GPS coordinates) is accurate" (burden can be met by testimony from a Google Earth programmer, by witness who works with and relies on program, or judicial notice of program's reliability). For further discussion, *see* Mueller & Kirkpatrick, Federal Evidence [4th ed] Sec. 8:13.

3. On the other hand, computer stored records when their contents are being offered "for the truth" are considered to be hearsay, *e.g.,* printout describing observations of fact where the underlying date is not admitted. Thus, they are admissible only if an exception is present.

(a) Ordinarily, they are admitted as records of a generally conducted business under the applicable business records exception, *e.g.* FRE 803(6). In that regard, it is well established that computer stored records fall within that exception. (*See e.g., Ed Guth Realty, Inc. v. Gingold*, 358 N.Y.S.2d 367, 371 [1974]; *Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.*, 38 F.3d 627 [2d Cir. 1994]; *United States v. Moore*, 923 F.2d 910 [1st Cir. 1991]; *Sea-Land Serv., Inc. v. Lozen Intl.*, 285 F.3d 808, 819-820 [9th Cir. 2002]).

(b) The courts for the most part apply the usual foundation requirements (*see, e.g., United States v. Kassimu,* 188 Fed. Appx. 264 [5th Cir. 2006] [To authenticate computer records as business records did not require the maker, or even a custodian of the record, only a witness qualified to explain the record keeping system of the organization to confirm that the requirements of FRE 803(6) had been met, and the inability of a witness to attest to the accuracy of the information entered into the computer did not preclude admissibility]; *Ed Guth Realty, supra*; *United States v. Salgado*, 250 F.3d 438 [6th Cir. 2001]). However, some courts have articulated elements specifically for computer records. The reason is concern as to what has, or may have, happened to the record in the interval between when it was

placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created. Thus, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created. (*See, e.g., United States v. Cestnik*, 36 F.3d 904, 909-910[10th Cir. 1994][created for motives that tend to assure accuracy]; *In re Vinhee*, 336 B.R. 437, 447 [9th Cir. 2005][requiring foundation proof for 11 elements including proof that the computer is reliable]; Imwinkelried, Evidentiary Foundations at § 4.03[2]). To the extent a court may require proof of the reliability of the computer system, reliability can be shown by proof of a company's reliance upon the record. (*Salgado, supra*; Park, Evidence Law [4th ed.] Sec. 11:11)

.

(c) The foundation can be shown, as set forth in FRE 803(6), through testimony or by a certification complying with FRE 902(11) or 18 US.C. § 3505 that the records were contemporaneously made and kept in the normal and ordinary course of business by a person with knowledge. The requirement that the record be kept in the course of a regularly conducted business activity refers to the underlying data, and not the actual printout of that data. (*See, United States v. Fujii*, 301 F.3d 535 [7th Cir. 2002]).

(d) The printout, although produced in anticipation of litigation, is still within the exception. (*See, Ed Guth, supra*; NY CPLR 4518[a]; *United States v. Sanders*, 749 F.2d 195, 198 [5th Cir. 1984]).

4. The "public records" exception, statutory or common law, may also be used with respect to government computer records. (*See, e.g.,* FRE 803[8]; *Hughes v. United States*, 953 F.3d 531, 540 [9th Cir. 1992]; CPLR 4520; *Consolidated Midland Corp. v. Pharm. Corp.,* 345 N.Y.S.2d 105 [2d Dep't. 1977] [common law]).

C. Foundation: Authentication

1. As with other documents and other types of non-testimonial proof, computer records, whether computer generated or computer stored, must be authenticated, *i.e.,* the record is what its proponent claims it to be.

(a) The standard for authenticating computer records is the same as for authenticating other records. (*See, United States v. Simpson*, 152 F.3d 1241, 1249-1250 [10th Cir. 1998]; *In re F.P.*, 878 A.2d 91, 95-96 [Pa. Super. Ct. 2005]).

(b) As noted by CCIPS, generally authentication is generally accomplished through a witness who has first-hand knowledge of the facts, and how it was obtained from the computer or whether and how the witness's business relies upon the data. (*See*, *United States v. Salgado*, 240 F.3d at 453; *United States v. Moore*, 923 F.2d 910, 014-915 [1st Cir. 1991] [head of bank's consumer loan department could authenticate computerized loan data). Instead, the witness simply must have first-hand knowledge of the relevant facts, such as what the data is and how it was obtained from the computer or whether and how the witness's business relies upon the data]). It is not necessary that the computer programmer testify or that the witness called have special knowledge about the technical operations of the computer. (*Ibid.*).

2. When computer-stored records are being introduced and they are the records of regularly conducted business activity, FRE 902(11) (domestic records) and FRE 902 (12) (foreign records) and its state counterparts permit the use of a written certification in compliance with FRE 803(6) to establish the authenticity of the record. Additionally, FRE 901(b)(9) and its state counterparts permits evidence that the "process or system" for digitizing and maintaining the integrity of the records is accurate/reliable as a means of authentication.

3. When computer generated records are being introduced, FRE 901(b)(9) and its state counterparts also become applicable. (*See* CCIPS at p. 200). Additionally, as noted in CCIPS: "In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. *See, e.g., United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001) ("evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business" was sufficient for establishing trustworthiness); *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) ("[T]he ordinary business circumstances described suggest trustworthiness, . . . at least where absolutely nothing in the record in any way implies the lack thereof.")." (CCIPS, at pp.200-201; *see also, Brown v. Texas*, 163 S.W.3d 818, 824 (Tex. App. 2005) (holding that witness who used global positioning system technology daily could testify about technology's reliability).

(a) In *Ly v. State* (908 SW2d 598 [Tex. App. 1995]), the court upheld the admissibility of an automated computer monitoring printout regarding a person released on bail with specified conditions. At trial, Poole, the person who oversaw the system, testified to the reliability and accuracy of the electronic monitoring system. She further testified that Digital Products Corporation, the vendor and manufacturer of the electronic monitoring equipment, was also contacted on June 20th to verify that the electronic equipment was operating properly. Patton's testimony established that the monitor was trustworthy with respect to the information which appeared on the computer printout and that the computer was working properly when the printout was generated. Moreover, no controverting evidence was offered by appellant to indicate that the computer was not reliable or was not operating properly when the printout was generated. On this proof the Court concluded the State adequately proved the reliability of the computer printout.

(b) Also, evidence that a computer program is sufficiently trustworthy so that its results qualify as business record should in any event suffice to establish the requirement.

4. Effective December 1, 2017, FRE 902 was amended to add two provisions that permit self-authentication of computer records by certification.

(a) FRE 902(13) permits use of a certification to authenticate evidence generated by an electronic process or system, e.g., computer generated information. (*See generally,* Grimm *et al*, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 38-46 [2017]*; see also*, Practical Lawyer Litigation FRE 902 (13) sample certification (available on Westlaw).

(b) FRE 902 (14) permits use of a certification to authenticate "[d]ata copied from an electronic device, storage medium, or file." (*See generally,* Grimm *et al*, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 38-46 [2017]).

5. Lastly, it should be observed that the mere possibility that the record could easily be altered, *i.e.*, a single keystroke, does not affect the authenticity of a computer record. (*See, United States v. Whitaker*, 127 F.3d 595 [7th Cir. 1997]; *United States v. Glasser*, 773 F.2d 1553 [11th Cir.

1985]). However, the Manual for Complex Litigation cautions as follows: "Computerized data raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy." (Manual, §11.447 [4th ed]).

D. Foundation: Best Evidence

1. The original "writing" of these computer records is, strictly speaking, the collection of 0's and 1's. Hence, the mere printout of the record may not be the "original" for best evidence purposes.

2. FRE 1001(3) and state codifications derived from the FRE or specific state statutes, *see* NY CPLR 4518(a) and 4539(b), address this concern. These provisions recognize that "if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is an original." (FRE 1001[3]; *see, Briar Hill Apartments Co. v. Teperman*, 568 N.Y.S.2d 50, 52 [App. Div. 1991]).

E. Medical Records

1. Generally

(a) Health care professionals under the impetus of federal legislation have now transitioned to electronic medical records. (Health Information Technology for Economic and Clinical Health Act, Pub L. No. 111-5, 123 Stat. 115, 226 (2009); *HITECH Act Enforcement Interim Final Rule*, U.S. DEPARTMENT OF HHS, https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/).

(b) As an authoritative commentary has noted: "An electronic or computerized medical record is a digital version of the patient's paper chart and represents a medical record for a single facility, such as the family doctor, group practice, or hospital. The electronic record will include such things as biographical information, the patient's past medical history, test results including blood and diagnostic studies, summaries of office visits, and other information relevant to the person's health. The document

may also include reports or encounters with other healthcare providers. In turn, these records are organized in a data-gathering configuration that allows for the retention and transfer of confidential health information in a protected fashion." (Hodge, Understanding Medical Records in the Twenty-First Century. 22 Barry L.Rev. 273, 274 [2017]).

(c) Admissibility is governed by the foundation elements above. However, many states have or are about to enact statutes that govern admissibility of electronic medical records. (*See* Hodge, *supra* at 289-293).

(d) For a discussion of the problems that can arise with electronic medical records, *see* Curran and Berman, Gremlins and Glitches, 85 NYSBA J. (May 2013), p. 20).

2. Audit Trail

(a) An audit trail is a form of metadata created as a function of the medical provider's computerization of medical records. One commentator described it as follows: "The audit trail is a document that shows the sequence of events related to the use of and access to an individual patient's EHR ["electronic health records"]. For instance, the audit trail will reveal who accessed a particular patient's records, when, and where the health care provider accessed the record. It also shows what the provider did with the records — e.g., simply reviewed them, prepared a note, or edited a note. The audit trail may also show how long the records were opened by a particular provider. Each time a patient's EHR is opened, regardless of the reason, the audit trail documents this detail. The audit trail cannot be erased and all events related to the access of a patient's EHR are permanently documented in the audit trail. Providers cannot hide anything they do with the medical record. No one can escape the audit trail." (2011 Health L. Handbook § 10:9). For further discussion, *see* Blind, The Electronic Health Record: A Discovery and Production Nightmare, 58 Univ Louisville L. Rev. 303 (2018).

(b) Federal law and many states that any medical provider who maintains electronic records must also maintain an audit trail (*see* 42 C.F.R. § 164.312; 10 NYCRR 405.10).

(c) As to discovery of audit trails, this issue was fully explored in *Gilbert v. Highland Hosp.* (31 NYS3d 397 [Sup.Ct. 2016]). The court granted plaintiff's application to compel discovery of the audit trails of

decedent's medical records, a form of metadata that would show the sequence of events related to the use of and access to decedent's medical records. It noted plaintiff's request was relevant to the allegations made in the complaint that decedent was not seen or evaluated by a medical doctor prior to her discharge from defendant. While the audit trails would not demonstrate all of the efforts of the emergency room attending physician, it would account for the attending physician's accessing and viewing decedent's electronic records, a topic that plaintiff may wish to explore further during a deposition or cross-examination, and should be considered material and necessary. Plaintiff's request could not be considered a fishing expedition as plaintiff knew the audit trails must exist, because they are mandated by law, and requested them for the specific reason of quantifying the level of involvement of the emergency department attending physician with decedent's care. Finally, plaintiff was not required to make a showing that the medical records already produced were not authentic, as system metadata is additionally relevant where it is important to the claims of a party to establish who received what information and when. *See also Vargas v. Lee*, 2019 WL 1271883 (2d Dept. 2019).

II. EMAILS

A. Foundation: Authentication

1. Emails and text messages when offered into evidence must be authenticated, namely, the proponent of the email must establish that the email is an email sent or received by the person or entity claimed to have sent or received it.

(a) The authentication of emails involve the same methods that are acceptable means of authenticating writings and other proffered evidence. (*See, US v. Gagliardi,* 506 F.3d 140, 151 [2d Cir. 2007]; *U.S. EEOC v. Olsten Staffing Serv. Corp.*, 657 F.Supp.2d 1029, 1034 [WD Wisc. 2009][rejecting argument that an email can only be authenticated by the author of the email]). These methods are delineated in FRE 901(b). (*See generally,* Grimm, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 12-18 [2017]).

(b) The mere possibility of the alteration of an email or the creation of a fraudulent email will not bar the admissibility of an email "any more than it can be the rationale for excluding paper documents." (*United*

States v. Safavian, 435 F. Supp.2d 36, 42 [D.DC 2006]; *Interest of F.P.*, 878 A.2d 91 Pa. Super. 2005]).

(c) The authentication process does not require the proponent of the email to disprove the possibility that a party or non-party altered the email. ((*Linde v. Arab Bank, PLC*, 97 F.Supp.3d 287, 337 [ED NY 2015])

(d) Where it can be established that the email was the product of computer error, it has been held that email will be deemed inadmissible. *See, Ermolaou v. Flipside, Inc.*, 2004 WL 503758, at *6 [S.D.N.Y.][computer glitch resulting in erroneous notification]).

2. Authenticity can be established by testimony of the person who sent or received the email, essentially, the email is the personal correspondence of the person. (*See, United States v. Fluker,* 698 F3d 988, 999 [7th Cir. 2012]; *Ryan v. Shawnee Mission Unified School Dist.*, 437 F.Supp.2d 1233, 1235-1236 [D Kan. 2006]; *Petroleum Sales, Inc. v. Valero Refining Co.*, 2006 WL 3708062 [N.D. Cal.]; *U.S. EEOC v. Olsten Staffing Serv. Corp., supra; Tibbetts v. Radioshack Corp.,* 2004 WL 2203418, *13 [ND Ill.]["true copies of his own correspondence"]).

3. In the absence of testimony from the person who sent the email, it must be kept in mind that merely because the email purports to come from the email address in the sender box is generally insufficient to authenticate the message as being sent from the indicated person. There must be some confirming circumstances – circumstantial evidence – sufficient to establish by the claimed person or entity. (*See, People v. Agudelo,* 947 NYS2d 96 [NY App. Div. 2013]; *People v. Hughes*, 981 NYS2d 158 [NY App. Div. 2014]; *Commonwealth v. Purdy,* 945 N.E.2d 372, 382 [Ma. 2011]; *Lorraine v. Markel Amer. Ins. Co.,*241 F.R.D. 534, 555 [D Md. 2007]; *see, also,* Broun, McCormick on Evidence [7th ed] §227 at p. 103; Joseph, "What Every Judge and Lawyer Needs to Know About Electronic Evidence," 99 Judicature 48, 53 [2015]). However, with respect to email alleged to have originated from a business, it has been held that the name of the business (in full or abbreviated) in the email sender address after the @ symbol is presumably from the business. (*Superhighway Consulting Inc. v. Techwave, Inc.,* 1999 US Dist. LEXIS 17910 at *6 [ND Ill.] [citing to FRE 902[7]).

4. Circumstantial Evidence

(a) The contents reveal matters known only by the sender or a small group of persons. (*See e.g., Lorraine,* 241 F.R.D. at 554; *United States v. Siddiqui,* 235 F.3d 1318 [11th Cir. 2002]; *State of Arizona v. Damper,* 225 P.3d 1148[Ariz. App. 2014]; *Dickens v. State,* 927 A.2d. 32 [Md. App. 2007]; *Massimo v. State*, 144 SW3d 210 [Tex. App. 2004]).

(b) The address of the recipient is consistent with the email address on other emails sent by the same sender. (*Shea v. State*, 167 S.W.3d 98, 105 [Tex. App. 2005]).

(c) The email contains "distinctive characteristics," such as unique word choice, special font, emoji, which are commonly used by or associated with the alleged sender, electronic signature of the sender (*Safavian, supra*, at 40; *Siddiqui, supra*, at 1322; *United States v. Brinson*, 772 F3d 1314 [10th Cir. 2014] [alias used by defendant]; *State v. Pullens*, 800 NW2d 202, 229 [Neb. 2011]).

(d) Reliance upon the "Reply Letter" rule or on-going exchange of emails. (*See, Varkonyi v. State,* 276 S.W.3d 27 [Tex. App. 2008]; *Manuel v. State*, 317 SW3d 66 [Tex. App. 2011]; *Safavian,* 345 F.Supp.2d at 42).

(e) Subsequent conduct of the person showing awareness of the contents, such as acting consistent with it. (*See, Commonwealth v. Czubinski,* 26 N.E.3d 753 [Mass. App. Ct. 2015]; *State v. Ruiz*, 2014 WL 2040016 [Mich. Ct. App]).

(f) Found on alleged sender's computer in "Sent" file with the same date/time on it. (*See, State v. Burns*, 2015 WL 2105543 at *11 (Tenn. Crim. App]).

5. If the email is produced by a party from the party's files in the course of discovery, the act of production can serve as proof of authentication. (*See, Nola Fine Art, Inc. v. Ducks Unlimited, Inc.*, 88 F.Supp.3d 602 [ED La 2015 ["Defendant produced the email to plaintiffs in discovery and therefore cannot seriously dispute the email's authenticity."]; *Schaghticoke Tribal Nation v. Kempthorne,* 587 F.Supp.2d 389 [D. Conn. 2008]; *Perfect 10, Inc. v. Cybernet Ventures, Inc.,* 213 F.Supp.2d 1146 [CD Cal.2002]; *Dominion Nutrition, Inc. v. Cesca*, WL 560580 *5 [N.D.Ill.]). However, authentication is not established when

email is offered by the producing party. (*See, Eastview Healthcare, LLC v. Synertx, Inc.*, 298 Ga. App. 393, 674 S.E.2d 641 [2009]).

6. Information obtained from ISP and forensic testimony, including email's hash values and connecting the email to sender's computer.

7. As to attachments, in *Madison One Holdings, LLC v. Punch Intern., NV* (2009 WL 911984 at *11 [SD Tex]), it was held that attachments to authenticated emails are themselves authenticated.

B. Foundation: Hearsay

1. When proffering emails as evidence, the hearsay rule is implicated, just as it would be with hand-written correspondence. (*See, CA, Inc. v. Simple. com*, 2009 US Dist. LEXIS 25242, *57 [SDNY]). If the email is being admitted for its truth, it is barred by the hearsay rule unless an exception is present; and if it is not being offered for the truth, the hearsay rule is inapplicable. (*See, U.S. EEOC v. Olsten Staffing Serv. Corp.*, 657 F.Supp.2d 1029, 1035 [WD Wisc. 2009]; *Houd-O'Hara v. Wills*, 873 A.2d 757, 760 [Pa. Super. 2005]).

(a) Where the proffer is an email chain, each email must be separately analyzed. (*See, In re Processed Egg Prods. Antitrust Litig.*, 2018 WL 1725802 [ED Pa]).

(b) For an excellent discussion of various issues as to how emails might fit within the hearsay exceptions, *see*, Belin, eHearsay, 98 Minn. L. Rev. 7 (2013).

2. Exceptions

(a) Admissions

(i) Where the sender is a party-opponent, the email is admissible under the admissions exception. (*See, e.g., United States v. Siddiqui*, 235 F.3d 1318, 1323 [11th Cir. 2000]; *United States v. Sprick*, 233 F.3d 845, 852 [5th Cir. 2000]; *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146, 1153 [C.D. Cal. 2002][employee admission]; *U.S. EEOC v. Olsten Staffing Serv. Corp., supra* [employee admission]).

(ii) An email forwarded by a party opponent may constitute an adoptive admission of the email. (*See, Sea-Land Serv., Inc. v. Lozen Int'l. LLC*, 285 F.3d 808, 821 [9th Cir. 2002]; *United States v. Safavian*, 435 F.Supp.2d 36, 43-44 [S.D.N.Y. 2006]).

(b) Present Sense Impressions and Excited Utterances

(i) In *United States v. Ferber* (966 F.Supp. 90 [D. Ma. 1997]), court admitted an email from a subordinate to his superior describing telephone conversation with defendant who was not a fellow employee as a present sense impression. (*See also, State of New York v. Microsoft Corp.*, 2002 WL 649951, *2 [D.D.C.][finding the exception inapplicable]). Similarly, an email may constitute an excited utterance. (*See State v. Cunningham*, 40 P.3d 1065, 1076 n. 8 [Ore. 2002]).

(c) State of Mind

(i) Where a party's state of mind is relevant, an email may be admissible to show the recipient's state of mind at the time received. (*Safavian, supra*, at 44). Email can also be used to prove the author's state of mind as non-hearsay. (*See, U.S. v. Brown*, 459 F.3d 509, 528, n. 17 [5th Cir. 2006]).

(d) Business Record

(i) Email *may* constitute a business record. (*See generally, In Re Oil Spill by the Oil Rig "Deepwater Horizon,"* 2012 WL 37373, at *4-7 [ED La]). However, just because the email was made by an employee does not automatically make it a business record. (*United States v. Cone*, 714 F3d 197 [4th Cir. 2013]). As stated in *Lorraine*: "It is essential for the exception to apply that it was made in furtherance of the business needs, [and] not for the personal purposes of the person who made it. Given the fact that many employees use the computers where they work for personal as well as business reasons, some care must be taken to analyze whether the business record exception is applicable, especially to email." (*Lorraine, supra*, 241 F.R.D. at 571). In *Goss v. Tommy Burney Homes, Inc.* (2009 WL 2868765 [Tenn. Ct. App.]), trial court admitted several emails between employees of defendant – Barnes and Burney – which were offered by defendants as business records. Court held the emails were properly admitted. It noted:

"In laying the foundation for introducing the emails, Ms. Barnes testified that she and Mr. Burney had worked together for more than ten years and had discovered during that time that it was critical to the success of a project that they document the process including interactions with home purchasers. As a result, they had established a system whereby they would communicate by email to each other and Ms. Barnes would print out all the emails related to a project and place them in the project file as a record. Mr. Burney confirmed this documentation and recording system in his testimony. The emails themselves also confirm this system of record-keeping as many of them state that the email is for the purpose of "documenting for the file." The evidence supports the conclusion that these were business records and properly admitted."

(ii) Where it is not shown that it was the regular practice of the employer to require that the employee make and maintain emails or that it was the regular practice of the employee to write and maintain emails, the basic foundation requirements have not been met. (*See, State of New York, supra*, *1; *Ferber, supra*, at 98-99).

(iii) "The fact that an employee 'routinely' takes meeting notes and keeps them is quite different than whether a company policy directs the employee to do so." (*Rambus, Inc. v. Infineon Technologies AG*, 348 F.Supp.2d 698, 705-706 [E.D.Va. 2004]).

(iv) An admissibility obstacle may also be present when "email chains" are offered and the "chain" email has been created in the course of another entity's business. (*Rambus, supra*, at 706).

(e) "Double-hearsay" in emails must also be addressed and there must be a showing that each level of hearsay is covered by an exception or that it is being offered for a non-truth purpose. (*See, Trade Finance partners, LLC v. AAR Corp.*, 2008 WL 904885, *8 [NO Ill.], *affd.* 573 F.3d 401 [7th Cir. 2009]; *State of New York v. Microsoft, supra*, at *3; *In re Oil Spill by Oil Rig "Deepwater Horizon", supra).*

C. Foundation: Best Evidence

1. The best evidence rule will as a general proposition not be a bar to the admissibility of emails, as the electronic files, not the printouts from the message logs, are considered the "originals". (FRE 1001[3]; *Abrams v. State*, 117 P.3d 1210 [Wyo. 2005]).

2. Testimony or other evidence to establish the contents of the message will be admissible where the "original" is not available either because it cannot be located or it has been destroyed, and good faith is present regarding same. (*See, United States v. Culberson,* 2007 WL 1266131 [ED Mich.]; *State v. Espiritu*, 117 Haw. 127, 176 P.3d 885 [2008]).

III. TEXT MESSAGES

A. Generally

1. While text messages are becoming more and common, there is as compared to emails a less developed body of case law addressing their admissibility. However, as they are fundamentally similar in kind to emails, the same basic rules applicable to emails will apply to text messages. *(See, People v. Dixon*, 40 NYS3d 184 [App. Div. 2016]; *People v. Moye*, 2016 WL 1708504 [NY Sup. Ct. 2016]; *Manuel v. State*, 357 SW3d 66 [Tex. App. 2011]; *Commonwealth v. Mosely*, 114 A3d 1072 [Pa. Super. Ct. 2015]; Grimm, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 19-23 [2017]).

2. The Nebraska Court of Appeals noted in *State v. James* (2018 WL 1074879 [Neb. App]) that the proponent of the text messages is not required to conclusively prove who authored the messages before they can be admitted into evidence. Instead, the possibility of an alteration or misuse by another generally goes to weight, not admissibility."

3. Forensic proof should not be overlooked. (*See, United States v. Kilpatrick*, 2012 WL 3236727, at *3 [ED Mich.] [IT expert testified text message was collected from a server that is inaccessible to users and renders the stored messages unalterable]).

B. Chain of Text Messages

1. Courts uniformly hold as to admitting a chain of text messages, that each text message is generally treated as an individual record requiring separate foundation and grounds before being admitted. (*See, United States v. Ellis*, 2013 WL 2285457, at *2 [ED Mich.], *affd*. 626 Fed Appx. 148 [6th

Cir. 2015]; *United States v, Thomas*, 2015 WL 237337, at *4 [D. Conn]; *State v. Martinez*, 364 P3d 743 [Ore App. 2015]; *People v. Dixon*, 40 NYS3d 184 [App. Div. 2016]; *see generally*, Andoh and Salem, Text Messages as Evidence, NYLJ, Feb. 9, 2018, p3 col 3 [excellent discussion of the issue]).

IV. SOCIAL MEDIA POSTINGS

A. Generally

1. Social media was aptly described *in Parker v. State* (85 A.3d 682, 685 [Del. 2014]) as "forms of electronic communications ... through which users create online communities to share information, ideas, personal messages, and other content (as videos). Through these sites, users can create a personal profile, which usually includes the user's name, location, and often a picture of the user. On many sites such as Facebook or Twitter, a user will post content — which can include text, pictures, or videos — to that user's profile page delivering it to the author's subscribers."

2. Often these posts will include relevant evidence for a trial, including party admissions, inculpatory or exculpatory photos, or online communication between users. Issues on admissibility will then arise.

3. " But there is a genuine concern that such evidence could be faked or forged." (*Id.*).

4. These matters were present in *United States v. Zayner* (769 F3d 125 [2d Cir. 2014]. In this case Zhyltsou was charged with transfer of a false identification document. To prove the charge, the government offered into evidence a printed copy of a web page, which it claimed was Zhyltsou's profile page from a Russian social networking site akin to Facebook. The trial court admitted the page because it bore the name and picture of the purported owner Zhyltsou. Court reversed conviction, finding there was insufficient proof of authentication. In reversing, Court observed: "It is uncontroverted that information *about* Zhyltsou appeared on the VK page: his name, photograph, and some details about his life consistent with Timku's testimony about him. But there was no evidence that Zhyltsou himself had created the page or was responsible for its contents. Had the government sought to introduce, for instance, a flyer found on the street that contained Zhyltsou's Skype address and was purportedly written or authorized by him, the district court surely would have required some

evidence that the flyer did, in fact, emanate from Zhyltsou. Otherwise, how could the statements in the flyer be attributed to him?"

B. Authentication

1. Generally

(a) The traditional authentication rules apply to social media, encompassing the individual web page – profile – and posts on it, whether, written, photographs or videos, and messages thereon.

(b) Three steps are involved: (1) the printout or testimony describing what was viewed accurately reflects the computer image of the web page as of the claimed date; (2) the website where the posting appears is owned or controlled by the claimed person or entity; and (3) the authorship of the posting is reasonably attributable to that person. (*See generally,* Joseph, "What Every Judge and Lawyer Needs to Know About Electronic Evidence", 99 Judicature 49, 50 [2015]; *United States v. Vayner*, *supra*; *Griffin v. State*, 19 A.3d 415 [Md. 2011]).

(i) Step 1 can be established by the testimony of a witness that he or she logged on to the site, typing the URL associated with website; reviewed and read what appeared on the computer screen; and the printout or his or her testimony accurately reflects what he or she saw.

(ii) Step 2 can be established by admissions of the person or entity, evidence linking the URL to the person or entity, or consideration of distinctive characteristics shown by an examination of the website's contents and substance which links the website to the person or entity. Expert evidence may possibly be needed as well.

(iii) In the absence of testimony from a person involved in the posting, satisfaction of Step 3 requires careful consideration of authentication rules. The possibility of hacking has influenced the courts regarding their application.

2. Authorship (Step 3)

(a) Both the social media page and the post in issue must be

linked to the claimed author. (*United States v. Vayner*, supra at 131-132; Mueller and Kirkpatrick, Federal Evidence [4th ed.] §9:9; Joseph, *supra*, at p.51).

(b) This can be accomplished in a variety of ways in addition to a witness with personal knowledge or an admission. (FRE 901[b]). (*See*, Grimm, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 31-34 [2017]).

(i) Expert testimony derived from an examination of the claimed author's computer's or electronic device's Internet history and hard drive. (*See, People v. Clevinstine,* 891 NYS3d 511 [App. Div. 2009]).

(ii) Information from the social networking website that links the page to the claimed owner and links the post to that person. (*United States v. Siddiqui,* 235 F.3d 1318 [11th Cir. 2000]).

(iii) Circumstantial evidence such as testimony of a person that he or she frequently communicated with the claimed author through that page; the consistency of the post with another post made by the claimed author; claimed author's awareness of the conduct in issue as shown in the details of the post; the post's references to intimate pieces of knowledge or a little-known nickname; and consistency with prior or subsequent statements or conduct made by the claimed *author. (See, United States v. Vayner,* 769 F.3d at 130-131 [collecting cases]*; United States v. Siddiqui,* 235 F.3d 1318 [11th Cir. 2000]; *United States v. Hassan,* 742 F.3d 104 [4th Cir. 2014; *People v. Valdez,* 135 Cal. Rptr.3d 628 [2011]; *People v. Pierre,* 838 NYS2d 546 [App. Div.2007*]; Tienda v. State*, 358 S.W.3d 633 [Crim App. Texas 2012]["individualization of comments"]; Raysman and Brown, "Authentication of Social Media Evidence," NYLJ, 11/11/11, p. 3, col. 1; Joseph, *supra*, pp. 51-52).

(iv) Some commentators, but not all, have viewed the state of law regarding authentication as "murky at best," finding different approaches. (*See*, Angus-Anderson, "Authenticity and Admissibility of Social Media Website Printouts," 14 Duke L.& Tech. Rev. 33, 37 [2015]).

(v) In *Griffin v. Maryland* (19 AD3d 415 [Md. Ct. App. 2011]), the Court held selected printouts from a MYSpace page, utilized to show that a key witness had been threatened, had not been properly authenticated. A three-method proposal was set forth: "The first,

and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question, i.e. "[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be." The second option may be to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question. A third method may be to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it." (*See also Sublet v. Maryland*, 113 A3d 695 [Md. Ct. App. 2015] [applying *Griffin* to Tweets]). Of note, an appellate court in new Jersey held the three methods set forth in *Griffin* were too strict, and that they were not the only methods available for application. (*State v. Hannah*, 151 A3d 99 [App. Div. NJ 2016]).

(c) Where the post involves a photograph or video, such as a YouTube video, the foundation will require the usual showing that it is a fair and accurate representation of the individual and items depicted. (*See, United States v. Broomfield*, 591 Fed. Appx. 847 [11th Cir. 2014]). As stated in *United States v. Thomas* (701 Fed. Appx. 414 [6th Cir. 2017]): "A district court does not abuse its discretion when it admits social-media photographs that are offered into evidence after testimony that the photographs are what the proponent claims them to be. Here, that meant admitting the photographs after hearing testimony that the photographs to be admitted were indeed the photographs downloaded by the law-enforcement officers who found them. And the district court here — after considering the testimony of officers Holt and Rienerth, and being able to look at Thomas and the photographs — did not abuse its discretion in admitting the photographs that Thomas challenges."

(i) In such situations, proof of the ownership of the site, *i.e.*, does the person purportedly depicted own the site, is not necessary. (*See, United States v. Thomas, supra*; *State v. Krause*, 2017 WL 4335250 [Ohio Ct. App. 2017]; *Lamb v. State*, 2018 WL 2049640 [Fla. Ct. App]; *compare People v. Price*, 80 NE3d 1005 [NY Ct. App. 2017] [suggesting proof of defendant's ownership of the social media site on which the photograph was posted is necessary]).

(ii) In *United States v. Hassan* (742 F.3d 104, 132-133 [4th Cir. 2014]), the defendant argued that several prosecution exhibits consisting of Facebook pages and the files embedded therein—including videos hosted on YouTube (and maintained by Google)—were not properly authenticated. Court rejected the argument, noting that in establishing the admissibility of those exhibits, the government presented the certifications of records custodians of Facebook and Google, verifying that the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities. According to those certifications, Facebook and Google create and retain such pages and videos when (or soon after) their users post them through use of the Facebook or Google servers.

C. Foundation: Hearsay

1. Posts on a social media site when offered for their truth will constitute hearsay. (*See, Miles v. Raycom Media, Inc.,* 2010 WL 3419438 [SD Miss.][statements on page made by third parties offered for their truth]; *Fairweather v. Friendly's Ice Cream*, 2014 WL 3699489, n. 11 [D Maine][in discrimination action discussion of whether purpose of social media posting that he was "sick and tired" of customer complaints was offered for a truth purpose]).

2. When being offered against the author, the admissions exception will be applicable. (*See, People v. Oyerinde,* 2011 WL 5964613 [Mich. Ct. App.]; *Johnson v. Ingalls,* 95 A.D.3d 1446 [NY App. Div 2012]; *Melody M. v. Robert M.,* 103 A.D.3d 932 [App. Div. 2014]; *Tienda v. State,* 358 S.W.3d 633 [Crim App. Texas 2012]).

3. Where the post consists of a photograph or digital image, the hearsay rule is not implicated. (*See, United States v. Cameron*, 762 F.Supp.2d 152, 157159 [D. Maine 2011]).

D. Best Evidence

1. For purposes of the best evidence rule, the ESI "original" will be "the readable display of the information on the computer screen." (*Lorraine, supra*, 241 F.R.D. at 577) and the admissible "duplicate" the email printout.

V. SOCIAL MEDIA AND CHATROOM "CONVERSATIONS"

A. Generally

1. Discussion here concerns social media posts and "chatroom" posts made by third-parties, and not the owners of the site.

2. Basically, the same foundation rules previously discussed apply to such postings or "conversations".

B. Authentication

1. As leading commentators have observed: "Simply to show that a posting appears on a particular user's webpage is insufficient to authenticate the post as one written by the account holder. Third party posts, too, must be authenticated by more than the names of the purported authors reflected on the posts." (Grimm, *et. al.*, Authenticating Digital Evidence, 69 Baylor L. Rev. 1, 22 [2017]).

2. Personal knowledge and the usual forms of circumstantial evidence are the main methods. Screen name evidence is helpful, whether in the form of testimony stating the purported author uses that name in other situations (*See People v. Pierre*, 838 NYS2d 546 [App. Div.2007]), as well as the purported author's computer account specifying that name. (*See United States v. Manning*, 738 F3d 937 [8th Cir. 2014]).

3. Forensic proof is also a viable method. (Grimm, *supra*, at p.23, noting evidence from the hard drive of the purported author's computer reflecting that a user of the computer used the screen name in question can be used).

4. The decision in *Matter of Colby II. (Sheba II.)* (43 NYS3d 587 [App. Div. 2016]) is instructive. In this parental termination rights action, based upon neglect and abandonment, the respondent parent proffered Facebook messages to the subject child. She utilized her adult son's Facebook account. Court held the messages were properly authenticated and should have been admitted by the trial court. It stated: "Respondent testified that she was present when her counsel printed the Facebook messages at his office, and that she reviewed the entire document to ensure that it was a full and complete copy. The aforementioned stipulation [child had contact with mother through Facebook and had sent Facebook messages] and

respondent's testimony, when combined with her adult son's testimony confirming that he had provided respondent with his account information, password and permission to use the account for communication with the child, constituted a sufficient foundation for the admission into evidence of the printed messages and her related testimony."

VI. WEBSITES

A. Generally

1. Businesses, governments, not-for-profit entities and individuals maintain websites and post information that may be relevant in litigation involving them or third-parties.

2. Difficulties can arise as the issue becomes one involving so-called historic information, *i.e.,* matter posted in the past on the website.

B. Authentication

1. Authentication of web pages offered into evidence involve the same inquiries outlined above with respect to social media websites. (*See, O'Connor v. Newport Hosp.*, 111 A.3d 317, 324 [RI 2015]; *Estate of Konell v. Allied Prop. & Cas. Ins. Co.,* 2014 US Dist. LEXIS 10183 [D. Ore.]; Mueller and Kirkpatrick, Federal Evidence [4th ed.] §9:9). They are:

(a) the printout or testimony accurately reflects the computer image of the web page as of the claimed date;

(b) the website where the posting appears is owned or controlled by the claimed person or entity; and

(c) the authorship of the posting is reasonably attributable to that person.

2. Step one can be established by the testimony of a witness that he or she logged on to the site, typing the URL associated with website; reviewed and read what appeared on the computer screen; and the printout or his or her testimony accurately reflects what he or she saw. (*See, Buzz Off Insect Shield, LLC v. S.C. Johnson*, 606 F.Supp.2d 571, 594 [MDNC 2009]; *Miriam Osborne Mem. Home Assn. v. Assessor of City of Rye,* 9 Misc.3d 1019, 1030 [Sup. Ct. Westchester Co. 2005] [Dickerson, J.]; Joseph, "What

Every Judge and Lawyer Needs to Know About Electronic Evidence", 99 Judicature 49, 50 [2015]).

3. Step 2 can be established by admissions of the person or entity, evidence linking the URL to the person or entity, or consideration of distinctive characteristics shown by an examination of the website's contents and substance which links the website to the person or entity. (*See, Metcalf v. Blue Cross/Blue Shield,* 2013 WL 4012726, at *10 [D. Or.]; *People v. Glover,* 2015 WL 795690 [Col. Ct. App.]).

4. Ordinarily, once steps 1 and 2 are established, courts generally will presume as reasonable that the posting on the website was placed there by the person who owned or controlled the website. (*See,* Joseph, *supra,* at p. 50; Scheindlin *et. al.*, Electronic Discovery and Digital Evidence (3rd ed.) p.1003).

5. When concerns are present as to whether the posting is attributable to the claimed person or entity, other factors should be considered. (*See, United States v. Jackson,* 208 F.3d 633, 638 [7th. Cir. 2000]; Joseph, *supra,* p.50). They include:

(a) length of time the posting was on the website;

(b) contents of the posting is of a type ordinarily posted on the website;

(c) claimed owner or others have published elsewhere the data contained, identifying the website as the source.

6. Testimony of the webmaster can be offered regarding the hacking into the website by the posting.

7. Where an archive service is utilized, *e.g.*, "Wayback Machine", there is a need for authentication by someone with personal knowledge of reliability of the archive service from which the webpage was retrieved. (*See, Specht v. Google, Inc.,* 747 F.3d 929, 933 [7th Cir. 2014]). FRE 902 (13) should also be considered.

8. Some courts have held that postings on government websites are self-authenticating under FRE 902(5). (*See, Williams v. Long,* 585 F.Supp.2d 679, 686-99 and n. 4 [D.Md. 2008] [collecting cases]).

C. Hearsay

1. Postings where offered for their truth will implicate the hearsay rule. (*See, United States v. Jackson*, 208 F.3d 633 [7th Cir. 2000]; *Osborn v. Butler*, 712 F. Supp.2d 1134 [D. Idaho 2010]).

2. Where the posting attributable to a party is being offered against the party, the admissions exception to the hearsay rule is applicable. (*See, Town of Bethel v. Howard,* 95 A.D. 3d 1489 [App. Div. 2012]; *Van Westrien v. Americontinental Collection,* 94 F.Supp 2d. 1087, 1109 [D. Ore. 2009]).

(a) If the posting were made under the traditional foundation requirements, there is no reason why the exception should not apply. (See, *Border Collie Rescue, Inc. v. Ryan*, 418 F.Supp.2d 1330, 1350 n.16 [M.D. Fla. 2006]).

3. Information posted on a government website may be admissible under the various public records exceptions recognized statutorily or under the common law. (*See, Tener Consulting Services, LLC v. FSA Main Street, LLC,* 2009 NY Slip Op. 50857[U][Sup. Ct. Westchester Co.]; *Johnson-Woodbridge v. Woodbridge*, 2001 WL 838986 at *4, 2001 Ohio App. LEXIS 3319 at *12-13 [Ohio App.]).

4. Postings of businesses on their websites, especially documents, may be admissible under the business records exception provided the basic foundation requirements are established. As noted by a commentary, each digital entry is itself a business record as it is a "data compilation in any form." (*See*, Scheindlin, Electronic Evidence and Digital Evidence [3d ed], at p.1010; *see also, United States v. Sanders*, 749 F.2d 195, 198 [5th Cir. 1984]; *United States v. Cataban*, 836 F.2d 453, 456-457 [9th. Cir. 1988]).

D. Best Evidence

1. For purposes of the best evidence rule, the "original" will be the readable display of the information on the computer screen" and the admissible "duplicate" the email printout.

VII. DIGITAL PHOTOGRAPHY

A. Generally

1. Digital photographs are made from images captured by a digital camera and loaded into a computer. (*See generally*, Long, *Complete Digital Photography* [3rd ed 2005], at pp. 11-14; Campbell, "Evidentiary Requirements for the Admission of Enhanced Digital Photographs, 74 Def. Couns. J. 12, 13-14 [2007]). Crisper images are produced by digital cameras as compared to film-based photography. ("Considering Digital Cameras for a Law Office", 21 No. 19 Lawyers PC, 7/1/04, p. 1).

2. A digital photograph can also be created through digitally converted images from film. (Joseph, "Digital Enhancement and Digital Photography", ACI-ABA Course of Study - Trial Evidence [Feb. 2008]). This processing is helpful where the photographic image is of low quality due to its blurriness or graininess and optical enlargement will not or cannot correct that situation. (*See*, Seltzer, "Digital Image Processing", 3 Trial Diplomacy J. No. 4, pp. 57-61 [Winter, 1980-1981]).

3. Software programs are available that can process the data contained in the digital photograph file to change the appearance of the captured image. (Campbell, *supra*,at p. 13-14). This "enhancement" consists of "removing, inserting or highlighting an aspect of the photograph that the technician wants to change." (Imwinkelried, "Can This Photo Be Trusted", Trial, Oct. 2005, at 48).

B. Hearsay

1. As with traditional photographs, digital photographs do not present hearsay concerns either because they are demonstrative in nature and do not make an assertion; or do not constitute a statement. (*See, United States v. Lizarraga-Tirado,* 789 F.3d 1107, 1109 [9th Cir. 2015]; *People v. Goldsmith*, 326 P.3d 239, 249 [Cal. Sup. Ct. 2014]; Martin, "Evidence", NYLJ, 2/13/09, p. 3, col.3).

2. The evidentiary concern involves the authentication rule, which will include the process by which the digital photograph was produced.

C. Authentication

1. Generally

(a) The proof that is necessary to authenticate a digital photograph or video will vary with the nature of the evidence that the photograph or video is being offered to prove and with the degree of possible error. (*See, People v. Goldsmith*, 326 P.3d at 245 [red light traffic camera]). However, no elaborate showing of accuracy is required. (*People v. Goldsmith*, 326 P.3d at 248).

(b) Digital camera's ability to manipulate images leads to the ability to easily alter the ultimate larger images. This ease is what creates authentication issues. (*See*, Rice, Electronic Evidence: Law and Practice [2d ed.], pp. 357-360).

2. Original Digital Photograph

(a) An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it. If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it." (*Lorraine, supra*, 241 F.R.D. at 562; *Almond v. State*, 274 Ga. 348, 349, 553 S.E.2d 803, 805 [2001]["the pictures were introduced only after the prosecution properly authenticated them as fair and truthful representations of what they purported to depict. . . . We are aware of no authority, and appellant cites none, for the proposition that the procedure for admitting pictures should be any different when they were taken by a digital camera"]).

3. Digitally Converted Image

(a) For digitally converted images, authentication "requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images, FRE Rules 901(b)(1) and 901(b)(9). Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo was produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion. (*Lorraine, supra*, 241 F.R.D. at 561).

4. Enhancement

(a) For digitally enhanced images, it has been observed that "it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified. In such a case, there will need to be proof, permissible under FRE 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence." (*Lorraine, supra*, 241 F.R.D. at 561). However, most courts have found digitally enhanced photographic evidence to be sufficiently reliable to meet the requirements of *Daubert* and/or *Frye*. (*See, State v. Hayden*, 950 P.2d 1024 [Wash. App. Div. 1998]; *Hartman v. Bagley*, 333 F.Supp.2d 632 [N.D.Ohio 2004]; *Campbell, supra*, at 14-16).

(b) In *State v. Swinton* (847 A.2d 921, 939-944 [Conn.2004]), the Connecticut Supreme Court adopted the following foundation standard: "(1) the computer equipment is accepted in the field as standard and competent and was in good working order, (2) qualified computer operators were employed, (3) proper procedures were followed in connection with the input and output of the information, (4) a reliable software program was utilized, (5) the equipment was programmed and operated correctly, and (6) the exhibit is properly identified as the output in question."

D. Best Evidence

1. The digital photograph will be viewed as the "original" for purposes of the best evidence rule where the photograph is not being used to illustrate and explain but for its independent probative value. (FRE 1001[3][4]; *Weinstein's Evidence Manual* [8th ed] §9.01[3], at pp. 9-7 to 9-8; *Bunting v. Sea Ray, Inc.*, 99 F.3d 887 [8th Cir. 1996]).

VIII. COMPUTER GENERATED ANIMATIONS AND SIMULATIONS

A. Generally

1. A computer animation is "the display of a sequence of computer-generated images." (Imwinkelreid, *Evidentiary Foundations* [6th ed 2005] §4:09[4][a]).

2. A computer animation can be used to analyze data, simulate fact patterns, illustrate and explain an expert's opinion. In essence, it is being utilized for demonstrative purposes, and when so used, it will simply be referred to as an "animation". (*See, e.g., Commercial Union Ins. Co. v. Boston Edison*, 591 N.E.2d 165 [Ma. 1992]; *Lally v. Volkswagen*, 698 N.E.2d 28 [2010]; *Mass. Port Auth. V. City of Boston*, 17 Mass. L. Rptr. 125 at 815 n.49 [Superior Ct. 2003]; *Kane v. Triborough Bridge & Tunnel Auth.*, 778 N.Y.S.2d 52, 55 [2d Dep't 2004]; *Lorraine, supra*, 241 F.R.D. at 559; *State v. Sayles*, 662 N.W.2d 1, 9 [Iowa 2003]). In *Verizon Directories v. Yellow Book USA* (331 F.Supp.2d 136 [EDNY 2004]), Judge Jack Weinstein expressed a position that favored computer-generated demonstrative exhibits, which h referred to as "pedagogical devices."

3. Where the animation is used substantively, *e.g.*, functions as an expert witness itself, it is referred to as a simulation. (*Sayles, supra*, at p. 9). It is so treated as it is "based on scientific or physical principles and data entered into a computer, which is programmed to analyze the data and draw a conclusion from it . . . . ." (*Lorraine, supra*, 241 F.R.D. at 559).

4. The classification of a computer-generated exhibit as an animation or simulation will determine the foundation required for it and its admissibility as well. In a leading case, the California Supreme Court in *People v. Duenas* (281 P3d. 887 (Cal. Sup. Ct. 2012]) described the differences as follows: "Animation is merely used to illustrate an expert's testimony, while simulations contain scientific or physical principles requiring validation. [Citation.] Animations do not draw conclusions; they attempt to recreate a scene or process, thus they are treated like demonstrative aids. [Citation.] Computer simulations are created by entering data into computer models which analyze the data and reach a conclusion." In other words, a computer animation is demonstrative evidence offered to help a jury understand expert testimony or other substantive evidence; a computer simulation, by contrast, is itself substantive evidence."

(a) Animations are subject to the rules governing use of demonstrative exhibits, whereas computer simulations are subject to a "more rigorous" scientific evidence standard. (See generally Hoenig, Admissibility of Computer Generated Animations, NYLJ, Jan. 5, 2018, p.3, col. 3 [discussing the cases]).

5. Due to the high potential for prejudice inherent in allowing a jury to view the animation, its admissibility is subject to the sound exercise of a trial court's discretion. (See, Kane, supra; Lorraine, supra).

6. For a collection of cases by federal circuit and state courts discussing the case law, see Webster and Bourn, The Use of Computer-Generated Animations and Simulations at Trial, 83 Defense Counsel Journal [October 2016] 439.

B. Hearsay

1. No hearsay issues are present as an animation is not being used to establish "truth" and a simulation is not generated by a person but by a machine.

C. Authentication

1. An "animation" can be authenticated by testimony that it fairly and accurately portrays the facts as testified to and that it will help to illustrate the testimony given in the action. (*See, e.g., Kane, supra; People v. McHugh*, 476 N.Y.S.2d 721 [Sup. Ct. Bronx Co. 1984]; *Sayles, supra*, 662 N.W.2d at 10; *Hinkle v. City of Clarksburg*, 81 F.3d 416 [4th Cir. 1996]; *People v. Cauley*, 32 P.3d 602 [Col. App. 2001]). In essence, nothing more complex than "Does this animation accurately reflect your testimony?" There is no need to show how computer-wise the animation was created, nor a need for a *Daubert* or *Frye* hearing. (*McHugh, supra*).

2. Concerning "simulations," it has been observed by a leading commentator that "a key test of admissibility is reliability, and a strong indicator or reliability is the extent to which a computer program that has been used to create evidence is accepted in the world of commerce and affairs - the relevant business, governmental, academic or other apt community. This reflects the practical test that the rules of evidence commonly employ – is the evidence sufficiently reliable that people rely on it to conduct their affairs outside of litigation? That entails the requirement that the mode is used in a manner consistent with its use by others in the field." (Joseph, "A Simplified Approach to Computer Generated Evidence and Animations," ALI-ABA Course of Study - Trial Evidence [Feb. 2008] [collecting cases]). A leading case, *Commercial Union v. Boston Edison* (591 N.E.2d 165 [Mass. 1992]), emphasizes that simulations should be treated like scientific tests.

D. Unfair Prejudice

1. "Unfair prejudice" arising from animations and simulations is a significant potential bar. (*Lorraine, supra*, 241 F.R.D. at 583-584). As one commentator has noted the significance of this evidence rule reemphasized by *Lorraine*: "The court furthermore explained that courts will be more likely to consider undue prejudice where there may be 'a substantial risk that the jury may mistake [the computer animations and simulations] for the actual events in litigation.' Most importantly, the court cautioned lawyers to be prepared to show why there is no unfair prejudice under Rule 403 when they are offering computer animations into evidence." (Kemp, "*Lorraine v. Markel*: An Authoritative Opinion", 9 NC J. Law and Tech. 16, 20 [2007]).

2. Two notable decision for comparison purposes *are Commonwealth v. Chukwuezi* (59 NE3d 380 [2016] [exclude]) and *Morency v. Annucci* (2017 WL 4417718 [ED NY] [admit]).

PART FOUR
JUDICIAL NOTICE

I. GENERALLY

A. Definition

1. Judicial notice of adjudicative fact is generally defined as the process by which a court accepts an adjudicative fact "as true without the offering of evidence by the party who should ordinarily have done so." (9 Wigmore, *Evidence* §2567, at 535 [3d ed.]).

2. Well established law limits the notice of adjudicative facts to facts incapable of serious dispute in that they are either generally known within the community where the trial court sits or capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. (*See,* FRE 201[b]; Broun, McCormick on Evidence [6th 3d] §§ 329-330).

3. The purpose of judicial notice is two-fold: (1) promote judicial convenience and efficiency so that time and resources are not wasted in proving facts that logic and experience dictate are true; and (2) keep juries

from making flagrant error through findings that are contrary to reality. As one treatise has aptly observed, judicial notice "controls the jury to prevent it from finding the world is flat, but also makes jury service more tolerable by not forcing the jurors to endure harangues from lawyers from the Flatlanders." (21 B Wright and Graham, Federal Practice and Procedure: Evidence (2d ed) §5102.2).

4. As can be readily observed, there are two significant tactical advantages to the party who persuades the court to take judicial notice of an adjudicative fact, especially in civil actions. First, judicial notice is a shortcut to proof, making unnecessary the calling of witnesses or admitting documentary evidence, thereby saving time and money. Second, in a civil action once a fact is judicially noticed, the opposing party cannot controvert that fact. Rather, the court instructs the jury to accept that fact as proved. As to this result, a commentator has cogently noted: "No mere witness could top the persuasive effect of the court stamping its seal of approval on a piece of evidence." (*See generally*, Dansky, "The Google Knows Many Things: Judicial Notice in the Internet Era," 39 Colorado Lawyer 19 [Nov. 2010]).

B. Application

1. Judicial notice can be taken at any stage of the action, including on appeal. (*See, e.g.,* FRE 201[d]; *Dippin Dots v. Frosty Bites Distrib.,* 369 F.3d 1197, 120401205[11th Cir. 2004]; *Hunter v. NY, Ontario & Western RR Co.*, 116 N.Y. 615, 23 N.E. 9 [1896][judicial notice taken on appeal]).

2. "It is a matter of common knowledge that courts occasionally consult sources not in evidence, ranging anywhere from dictionaries to medical treatises." (*Prestige Homes, Inc. v. Legouffe,* 658 P.2d 850, 854 [Col. 1983]).

3. The procedural incidents of taking judicial notice are set forth in FRE 201(c-e) and comparable state evidence codes.

4. While judicial notice is available in criminal cases, a jury will be instructed that it is not bound to accept the judicially noticed fact but that it may do so.

II. JUDICIAL NOTICE AND WEBSITES

A. Concern

1. May a court take judicial notice of adjudicative facts found on websites? In the absence of any statute or legal rule prohibiting courts from taking judicial notice of information found on the Internet, there is no reason why courts may not utilize websites as the source for facts of which they are taking judicial notice, provided the website can be deemed to be an "accurate" source. (*See*, Coleen Barger, *On the Internet, Nobody Knows You're A Judge: Appellate Courts' Use Of Internet Materials*, 4 J. App. Prac. & Process, 417, 431-432 [2002]).

2. The difference in the medium containing the information, one hard copy and the other electronic format, is no reason to treat these sources differently. To be sure, many websites cannot be viewed as reliable sources of information, but that problem is controlled by assessing on an individual basis websites and not by a blanket exclusion from judicial notice.

3. Of note, presently almost all courts have rejected a *per se* rule prohibiting the taking of judicial notice to facts found on websites. The views of judges expressing a declared distrust of such evidence when website derived evidence was first proffered in the 1990s, as exemplified by a judge who stated "any evidence procured off the Internet is adequate for almost nothing," are no longer in vogue.

B. Applied

1. As a result and in view of the relative ease of accessing information factual data and information on the Internet, judicial notice is frequently employed in litigation. (*See,* Bellin and Ferguson, "Trial by Google: Judicial Notice in the Information Age," 108 Nw. L. Rev. 1137 [2014]).

2. State and federal courts have taken judicial notice of facts found on websites. The websites utilized have included official government websites (*see, e.g., DeMatteo v. DeMatteo*, 749 N.Y.S.2d 671 [Sup. Ct. NY 2002][Julian, J.][Surgeon General for dangers of second-hand smoke]; *Tener Consulting Services, LLC v. FSA Main St., LLC,* 2009 NY Slip Op 50875[U][Scheinkman, J.][Secretary of State for "entity information" for plaintiff as to its principal place of business]; *Gent v. CUNA Mutual Ins. Co.,*

611 F.3d 79, 84 n. 5 [1st. Cir. 2010][Centers for Disease Control and Prevention concerning Lyme disease]; *Denius v. Dunlap*, 330 F.3d 919, 926 [7th Cir. 2003][National Personnel Records Center for records of retired military personnel]; *United States v. Bervaldi*, 226 F.3d 1256, 1266, n. 9 [11th Cir. 2000][U.S. Naval Observatory for time of sunrise]; *Levan v. Capital Cities ABC, Inc.*, 190 F.3d 1230, 1235, n. 12 [11th Cir. 1999][Federal Reserve Board for prime interest rate]).

3. Private and commercial websites – nongovernmental – have also been used for purposes of taking judicial notice by state and federal courts. (*See, e.g., People v. Clark,* 940 N.E.2d 755, 767 [Ill. App. Ct. 2010] [Google Maps for mileage distance]; *Ficic v. State Farm Fire & Cas. Co.*, 804 N.Y.S.2d 541 [Sup. Ct. NY 2005][Maltese, J.][Association of Arson Investigators for validity of arson investigation technique]; *Gallegos v. Elite Model Management Corp.*, 758 N.Y.S.2d 777 [Sup. Ct. NY 2003][hospital website for asthmatic conditions and causes]; *Schaffer v. Clinton,* 240 F.3d 878, 885 n. 8 [10th Cir. 2001] [political almanac for votes candidate received]; *Laborer's Persia Fund v. Blackmore Sewer Constr., Inc.*, 298 F.3d 600, 607 [7th Cir. 2002][bank for the bank's ownership]; *McCormack v. Heidman,* 694 F.3d 1004, 1008 n. 1 {9th Cir. 2012] [Google Maps for distance]; *Total Benefits v. Anthem Blue Cross*, 630 F. Supp. 2d 842, 849 [SD Ohio 2007[company website]).

4. Websites of commercial enterprises such as WebMD, which post information for use by the public and are readily accessible through Internet searches, and derive their income from such visits, will also be considered appropriate for judicial notice of its factual information. Likewise, judicial notice has been taken of facts on the websites of associations of professionals, and educational and medical providers. These websites are considered to be reliable sources as they all have an incentive to provide accurate information because if they provide inaccurate or incorrect information, loss of income to their sponsors, harm to the associations' members or harm to their reputation may occur.

5. In these decisions, the basic concern of the court was whether the website was a reliable source, as well as whether the information itself that was posted and retrieved was reliable. (*See,* Bellin, *supra,* 108 Nw. U. L. Rev. at 1164-1168]; *People v. Clark,* 940 N.E.2d at 767, *supra* ["mainstream websites"]). Where there are concerns as to reliability of the website or the information, judicial notice should not be taken. (*See,* Belin, *supra*, 108 Nw. L. Rev. at 1167-1180; *TR v. LVM*, 209 P.3d 879 [Wyo. Sup.

Ct. 2009][judicial notice of immunization schedule printed out from website would not be taken as the website was a unverified source and had not been authenticated by a medical expert and thus cannot be categorized as a source "whose accuracy cannot reasonably be questioned."]; *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 [3rd Cir. 2007][trial court should not have taken judicial notice of certain facts about plaintiff's business from website as it was "premature" to assume that the site was owned by the plaintiff and the website was used as a marketing tool and contained "puffery"]; *Miriam Osborne Memorial Hosp. Assoc. v. Assessor of the City of Rye*, 800 N.Y.S.2d 909 [Sup. Ct. Westchester Co. 2005][Dickerson, J.][court refused to take judicial notice of compilation of real property sales data from government website as the governmental entity attached to the compilation a disclaimer that it did not warrant "the accuracy, reliability or timeliness" of the underlying data comprising the compilation.]). Reliance on Wikipedia is controversial. (*See,*
Bellin, *supra,* 108 Nw. U. L. Rev. at 1164).

6. At a minimum, party asking a court to take judicial notice of information from a website should present to the court a printout of the relevant part of the website as well as the part showing date of last update (if available) and the date of the printout.

III. JUDICIAL NOTICE BY COURT *SUA SPONTE*

A. Concern

1. "Can judges appropriately conduct their own, independent Internet research as part of a beyond-the record "judicial fact-finding" effort? Should they be permitted to do so in order to better decide motions, cases and appeals before them? Is it proper for them to try to hunt down germane facts from, let's say, "highly reputable" websites or other Internet sources, or must judges render decisions based only on the record and showings made by the parties? Can judges properly "supplement" the facts before them from Internet sources as a form of assistance to decision-making?" (*See generally,* Hoenig, "When Judges Research the Internet", NYLJ, 1/11/16, p. 3, col. 3).

2. The various opinions in *Rowe v. Gibson* (798 F.3d 622 [7th Cir. 2015]) debate the issue. (*See also*, Thornburg, "The Lure of the Internet and the Limits on Judicial Fact Research," 38 Litigation 41 [2012]).

3. In Formal Opinion 478, dated December 8, 2017, the American Bar Association reviewed the ethical parameters under the Model Code of Judicial Conduct for conducting on-line independent fact-finding not tested by the adversary system.

B. Applied

1. When a court decides *sua sponte* to take judicial notice of a fact, the court should ordinarily advise the parties of its intent and request that the parties comment on it. (*See*, *Justice v. King*, 60 A.D.3d 1452, 876 N.Y.S.2d 301[4th Dep't. 2009]; George Marlow, *From Black Robes to White Lab Coats: The Ethical Implications of A Judge's Sua Sponte, Ex Parte Acquisition of Scientific Knowledge*, 72 St. John's L. Rev. 291 [1998]).

2. Suffice it to say that independent research on scientific issues by judges must be carefully weighed and considered. (*See*, Edward Cheng, *Research In The Daubert Age*, 56 Duke L. J. 1263 [2007]; Hall, "Should a Trial Judge Be permitted to Independently Google an Expert Witness to Determine Credibility," 112 Penn. St. L. Rev. 885 [2008]; *see also, Kiniti-Wairimu v. Holder,* 312 Fed. Appx. 907 [9th Cir. 2009] [finding a denial of petitioner's due process rights upon an Immigration Judge's independent research via the internet to obtain information used to make an adverse credibility determination]).

PART FIVE
ETHICS AND PRIVILEGE ISSUES

I. ETHICS

A. Basic Considerations

1. Competent Representation

(a) Model Rule of Professional Conduct (ABA) 1.1, Comment (8), as amended in 2012, provides "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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added)."

(b) Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained: " The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document."

2. Confidentiality

(a) Model Rule of Professional Conduct (ABA) 1.6, as amended in 2012, added a new duty in paragraph (c): "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

(b) Amended Comment [18] explains: "Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."

B. ABA Formal Opinion 477R (Revised May 22, 2017)

1. This Opinion defines the reasonable efforts standard for protecting client information as "reject[ing] requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

2. The Opinion provides several non-exclusive factors to be considered in determining reasonable efforts. They include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not

employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

3. As to what steps should be taken in a given set of facts, the Opinion offers several considerations as guidance lawyers should take to guard against disclosures, including: "1. Understand the nature of the threat. 2. Understand how client confidential information is transmitted and where it is stored. 3. Understand and use reasonable electronic security measures. 4. Determine how electronic communications about clients' matters should be protected. 5. Label client confidential information. 6. Train lawyers and nonlawyer assistants in technology and information security. 7. Conduct due diligence on vendors providing communication technology."

C. States

1. Nowadays, with the privacy of unencrypted email questioned after recent hacks, state bar association ethics opinions have begun to recommend encryption. (*See, e.g.,* State Bar of Texas Opinion 648 [July 2015]; State Bar of Pennsylvania Opinion 2011-200 [Nov. 2011]).

2. The circumstances delineated by the Texas Bar Ethics opinion: "communicating highly sensitive or confidential information via email or unencrypted email connections; sending an email to or from an account that the email sender or recipient shares with others; sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer."

II. METADATA

A. Generally

1. Metadata, frequently referred to as "data about data," is electronically stored evidence that describes the "history, tracking, or management of an electronic document" and includes the "hidden text, formatting codes, formulae and other information associated" with an electronic document. (The

Sedona Principles: Best Practice Recommendations for Document Production, Cmf. 12a [Sedona Conf. Group Series 2007]). Thus, metadata will include such information as the date the document was created, the author, and the date changes were made to the document.

2. Metadata is generated automatically by software. Most significantly, metadata in an electronic document can be "mined" or simply viewed by a recipient of the document by right-clicking a mouse or selecting "properties" or "show markup" on a Word document as well as with Excel and PowerPoint.

3. As a result, metadata can be harmful when users unknowingly send documents that contain confidential or potentially embarrassing information. (*See*, Farrar, "Metadata: The Hidden Disaster That's Right In Front Of You," 82 NYSBA J., Oct. 2010, p. 49).

B. Ethics Concerns

1. Most bar associations have issued opinions concerning metadata, addressing for the most part three issues: the sender's duty when transmitting metadata; recipient's ability to review or "mine" metadata; and obligation of the recipient to notify sender if metadata is found. However, these opinions take widely varying approaches. They are collected and discussed by the Law and Technology Resource Center of the ABA, which is available at https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.

2. As to some of the approaches:

(a) The American Bar Association has taken the position in Formal Opinion 06-442 (2006) that there is no ethical prohibition against an attorney accessing and using metadata embedded in electronic documents; and that to the extent an attorney is concerned about the disclosure of confidential information in metadata the attorney should employ a "scrubbing" program or other measures to prevent disclosure. Such other measures would include sending the document in a PDF format. (*Accord*, Maryland Ethics Op. No. 2007-09).

(b) The Minnesota Bar Association has opined that an attorney's obligation with respect to safeguarding information relating to the representation of a client against inadvertent or unauthorized disclosure

extends to metadata in electronic documents. (Minn. Lawyers Pro. Resp. Bd., Op. No. 22 [3/26/10]). Additionally, the Association opined that if a lawyer received a document which the lawyer knows or reasonably should know inadvertently contains confidential or privileged metadata, the lawyer shall promptly notify the document's sender as required by Rule 4.4(b), MRPC. (*Id.*). However, the Association did not address the question of "whether there is an ethical obligation on a receiving lawyer to look or not to look for metadata in an electronic document."

(c) In New York, the New York State Bar Association has taken the position in Opinion 749 (2008) that an attorney may not ethically use available technology to examine electronically transmitted documents. The New York County Lawyers' Association has concluded in opinion No. 738 (2008) that while attorneys are advised to take due care in sending correspondence, contracts, or other documents electronically to opposing counsel by scrubbing the documents to ensure that they are free of metadata, such as tracked changes and other documents property information, an adversary may not ethically take advantage of a breach in the attorney's care by intentionally searching for this metadata. The opinion states that using the metadata is unethical if the recipient's intent is to investigate opposing counsel's work product or client confidences or secrets or if the recipient is likely to find opposing counsel's work product or client confidences or secrets by searching the metadata. Using the metadata is appropriate in circumstances where the adversary has intentionally sent it such as where the lawyers are suing tracked changes to show one another their changes to a document. Without such prior course of conduct to the contrary, however, there is a presumption that disclosure of metadata is inadvertent and would be unethical to view. The NYSBA in Opinion 782 (December 2008) noted that attorneys have an ethical duty to "use reasonable care when transmitting documents by email to prevent the disclosure of metadata containing client confidences or secrets.

3. For a discussion of the "scrubbing devices" available, *see* Lukina, What's Hiding in Your Documents: The Dangers of Metadata, October 2017 NYSBA J. p. 46.

III. OTHER ELECTRONIC COMMUNICATIONS ISSUES

A. Privilege Concerns

1. Generally

(a) As a general proposition, privileged communications do not lose their privileged status merely because they are communicated electronically. (*See, e.g., McCook Metals, LLC v. Alcoa, Inc.,* 192 F.R.D. 242, 255 [ND Ill. 2000]; *United States v. Keystone Sanitation Co.*, 903 F.Supp. 803 [MD Pa. 1995]; *Steingart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. Sup. Ct. 2010); *see generally*, Note, "E-mail: The Attorney-Client Privilege Applied," 66 Geo. Wash. L. Rev. 624 [1998]; Fiocchi, Confidentiality and E-mail Communication: A Need for Clarification in Illinois Ethics Rules, 23 DCBA Brief 36 [October 2010]).

(i) Some states have enacted legislation so providing. (*See, e.g.*, NY CPLR 4548; Cal. Evid. Code §952).

(b) Communications that include third-parties outside of the attorney-client relationship are generally not privileged. (*See, e.g., Muro v. Target Corp.,* 243 F.R.D. 301, 307-310 [ND Ill. 2007]; *United States v. Chevron*, 241 F. Supp.2d 1065, 1076 n. 6 [ND Cal. 2002]; *United States v. Adlman*, 68 F.3d 1495, 1499 [2d Cir. 1995]; *People v. Mitchell*, 58 N.Y.2d 368, 373 [1983]).

(c) In *Willis v. Willis* (914 N.Y.S.2d 243 [App. Div. 2010]) the Court held the client's communication with her attorney with email account used by her children with her permission was not privileged as there was no expectation of confidentiality in these circumstances.

2. Third-Party Involvement

(a) Where the involvement of a third-party is necessary to aid the client in communicating or assist the attorney in performing legal services, such involvement does not defeat the privilege. (*See, United States v. Kovel*, 296 F.2d 918, 922 [2d Cir. 1961]).

(b) In *Green v. Beer* (2010 WL 3422723 [SDNY]), plaintiffs asserted the privilege with respect to email communications with persons who are neither attorneys nor parties to the litigation, namely, several

financial advisors and their son. Plaintiffs' financial advisors averred that they received particular emails from plaintiffs' counsel, and that they were assisting in the transmission of factual information between plaintiffs and plaintiffs' counsel. There was, however, no evidence that their involvement was necessary to ensure the provision of legal advice, or to facilitate the delivery of any emails. The son received email communications from counsel, which he then provided to his parents. He explained that his technical assistance was necessary for his parents to timely receive the email communications from counsel as they were not proficient in the use of the electronic mail. Court held that the emails disclosed to the financial advisors were not privileged as the sharing of them with those personas was not necessary to the provision of legal advice to the plaintiffs, but that the emails delivered through their son were within the privilege as the son's assistance was necessary.

3. Maintaining Confidentiality

(a) Waiver may occur when the privileged communication is carelessly left in a public or non-private location. (*See, Parnes v. Parnes*, 915 N.Y.S.2d 345, 349 [App. Div. 2011]).

(b) Waiver may also occur when user name and password to access email account containing confidential communications is left in a public area. (*See, Parnes,* 915 N.Y.S.2d at 349-350).

4. Attachments to Privileged Emails

(a) Merely attaching a document, including another email, to an email between client and attorney does not confer privileged status to that attached document as such a document is considered a pre-existing and thus not as a communication. (*See, Retail Brand Alliance, Inc. v. Factory Mut. Ins. Co.*, 2008 WL 3738979 at *4 [SDNY NY]).

5. Employee Use of Employer-Provided Computer

(a) Most courts hold that where an employee communicates with his/her attorney using the employer's provided computer and the employer has a written policy limiting the use of the computer to company business and/or the employer reserves the right to monitor usage, and thus the employee should not expect to have any personal privacy with respect to such usage, confidentiality does not attach to any attorney communications

to and from the attorney. (*See, Peerenboom v. Marvel Ent.,* 50 NYS3d 49 [App. Div. 2017]; *Scott v. Beth Israel Med. Ctr.*, 847 N.Y.S.2d 436 (Sup. Ct. 2007); *In Re Asia Glob. Crossing.*, 322 B.R. 24 [Bank. SDNY 2005]; *Kaufman v. SunGuard Inv.*, 2006 WL 1307882 (D N.J.); *In re Reserve Fund Securities Lit.*, 275 F.R.D. 154 (SD N.Y. 2011); *In re Royce Homes*, 449 B.R. 709, 732-744 (Bank. SD Tex. 2011); *see also, Convertino v. U.S. Dept. of Justice*, 674 F.Supp.2d 97 (D D.C. 2009) (absence of policy precluded a finding of no confidentiality); *see generally*, DeLisi, Employer Monitoring of Emails, 81 Ford. L. Rev. 3521 [2013])

(b) As to the use by the employee of the employee's own email account:

(i) In *Steingart v. Loving Care Agency, Inc.* (973 A.2d 390 [N.J. Super. A.D. 2009]), the Court refused to find a waiver where the employee was communicating with her attorney from a work computer through a personal password protected web-based email site, even though the employer had the ability to monitor those employee's emails. In so ruling, the Court rejected the employer's contention that its ownership of the computer was sufficient to establish ownership of the messages; expressed the view that access to the messages furthered no legitimate interest of the employer; and that in the circumstances the employee possessed a reasonable expectation that the messages would remain private. The Supreme Court of New Jersey affirmed these rulings, noting the employee's expectations of privacy were subjectively reasonable and the employee's efforts to protect confidentiality through using their own email account were objectively reasonable.

(ii) In *Miller v. Zara USA, Inc.* (56 NYS3d 302 [App. Div. 2017]), the employee, the company's General Counsel, retained personal documents on a company-owned laptop, but claimed that they were protected by the attorney-client privilege and the work-product doctrine. The company handbook specifically "restricted use of company-owned electronic resources, including computers, to 'business purposes"' and warned that "[a]ny data collected, downloaded and/or created" on such resources was "the exclusive property of Zara" and "may be accessed by Zara at any time, without prior notice." Contrary to *Stengart*, the Court held that, in light of the published company policy, the employee did not have a reasonable expectation of privacy with respect to those documents and therefore could not assert the attorney-client privilege.

B. Inadvertent Disclosure

1. Inadvertent disclosure of a confidential document in electronic form looms large in view of the extensive use of emails and the production of such documents in response to proper discovery demands. When the inadvertent disclosure involves a privileged document, whether it occurs in the context of litigation or a transactional matter, raises an issue as the possible loss of the privileged status pursuant to a waiver theory.

2. Three distinct approaches can be discerned in the situation where a party through its attorney or by itself inadvertently discloses to the adverse party a privileged document.

(a) One approach is that the inadvertent disclosure affects a waiver of privilege. (*See, e.g., SEC v. Lavin*, 111 F.3d 921 (D.C. Cir. 1997); *Carter v. Gibbs*, 909 F.2d 1450 (Fed. Cir. 1990); *FDIC v. Singh*, 140 F.R.D. 252 (D. Me. 1992); *Doe v. Maret*, 984 P.2d 980 (Utah 1999).

(b) A second approach is that an inadvertent disclosure cannot effect a waiver of the privilege.) *See, e.g., Leibel v. General Motors Corp.*, 646 N.W.2d 179 (Mich. Ct. App. 2002); *Harold Sampson Trust v. Linda Sampson Trust*, 679 N.W.2d 794 (Wisc. 2004). In the view of these courts, a waiver is present only through the client's intentional and knowing relinquishment of the privilege. *See, Gray v. Bicknell*, 86 F.3d 1472 (8th Cir. 1996)).

(c) The majority approach, and the approach followed in New York, is the use of a balancing test, which takes into account the precautions in place to prevent any inadvertent disclosure and the promptness of the party in asserting the privilege after the disclosure. (*See, e.g., Manufacturers & Traders Trust Co., 132 A.D.2d 392* [4th Dept.1987]; *Granada Corp. v. First Court of Appeals*, 844 S.W.2d 223 [Tex.1992]; *In re Copper Market Antitrust Lit.*, 200 F.R.D. 213 (S.D. N.Y. 2001]).

3. In 2008 the Federal Rules of Evidence were amended by the addition of FRE 502. This rule covers, among other matters dealing with the waiver of the attorney-client privilege, disclosure of otherwise privileged attorney-client communications and work-product protected documents which occurs during the course of a federal proceeding or to a federal agency or official. Comparable provisions have been enacted in many states.

(a) FRE 502(b) provides that a communication retains its protected status if "(1) the disclosure was inadvertent; (2) the holder of the privilege took reasonable steps to prevent disclosure; and (3) the holder took "reasonable steps to rectify the error, including (if applicable) following FRCP 26 (b)(5)(B)."

(b) FRE 502(b) adopts the third approach or middle-approach for inadvertent disclosure. The Commentary notes that this approach is in accord "with the majority view." While FRE 502(b) does not explicitly codify that approach, the Commentary states that the adopted approach's multifactor test for determining whether an inadvertent disclosure operates as a waiver has been "accommodated" through the Rule's flexibility. These factors, as set forth in the commentary, are the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure, and the overriding issue of fairness. (*See, Lois Sportswear v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 [S.D. N.Y. 1985]; *Hartford Fire Ins. Co. v. Garvey,* 109 F.R.D. 232, 332 [N.D. Cal. 1985]).

4. As to the ethical obligations of the recipient of an inadvertent email, FRCP(b)(5)(B) provides that in the absence of a confidentiality agreement where a receiving party is notified of the inadvertent disclosure by the adversary party, the recipient "must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim [of privilege] is resolved." The rule does not require the recipient to inform the adversary that it has apparently received privileged matter.

(a) There is no uniform position among bar associations regarding the ethical obligations of an attorney who inadvertently receives a privileged document.

(b) The American Bar Association has taken the position that an attorney who receives a document from another party and knows or reasonably knows that the document was inadvertently sent should promptly notify the sender in an order to allow the sender to take protective measures. (ABA Formal Op. 05-437 [2005]). ABA Model Rule 4.4(b) follows this opinion. Of note, a comment (2) to it, states: "Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document has been waived. Similarly, this Rule does

not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person."

(c) In New York, the Association of the Bar of the City of New York concluded in Formal Opinion 2003-04 that an attorney receiving a misdirected communication containing confidences or secrets (1) has obligations to promptly notify the sending attorney, to refrain from review of the communication, and to return or destroy the communication if so requested, but, (2) in limited circumstances, may submit the communication for *in camera* review by a tribunal, and (3) is not ethically barred from using information gleaned prior to knowing or having reason to know that the communication contains confidences or secrets not intended for the receiving lawyer. The opinion also states it is essential as an ethical matter that the receiving attorney promptly notify the sending attorney of the disclosure in order to give the sending attorney a reasonable opportunity to promptly take whatever steps he or she feels are necessary. The New York County Lawyer Association concluded in Formal Opinion 730 that if the attorney receives information which the attorney knows or believes was not intended for the attorney and contains secrets, confidences or other privileged matter, the attorney upon recognition of same, shall, without further review or other use thereof, notify the sender and (insofar as it shall have been written or other tangible form) abide by sender's instructions regarding return or destruction of the information. Of note, the opinion disagrees with the Association's view that a rule requiring attorneys who receive inadvertently disclosed privileged information without fault or misconduct on their part to refrain from reviewing inadvertently disclosed privileged information is required by DR 1-102(A)(4). In its view, an attorney does not "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation" under such circumstances.

(d) Several ethics opinions from other states have concluded that the attorney receiving the document has no obligation to disclose to the sender or to a court that the attorney possesses the document and the attorney may use the document. (*See, e.g.*, Kentucky Ethics Op. E-374 [1995]; Maine Ethics Op. No. 146 [1984]; Philadelphia Ethics Op. 94-3).

BIBLIOGRAPHY

Guide to New York Evidence

https://www.nycourts.gov/judges/evidence/index.shtml

Objective:

The objective of this Guide, as set forth in Rule 1.01,"is to bring together in one document, for the benefit of the bench and bar, New York's existing rules of evidence, setting forth each rule with a note on the sources for that rule. Given that most of New York's evidentiary rules are not codified and that the New York Court of Appeals provides the controlling interpretation of the New York State constitution, statutes and common law, this Guide places particular emphasis on, and adheres to, the controlling precedents of the New York Court of Appeals. Finally, the rules of evidence set forth in this Guide are not intended to alter the existing law of New York evidence and shall not be construed as doing so or as precluding a change in the law."

Committee:

Co-Chairs
Hon. William C. Donnino* Hon. Susan Phillips Read*

Reporter
Professor Michael J. Hutter
Albany Law School

Counsel

Shane T. Hegarty

Members

Hon. Lucy Billings	Hon. John Brunetti*	Hon. Fernando Camacho
Hon. Felix Catena	Hon. Mark Cohen	Hon. Daniel Conviser
Hon. Thomas Franczyk	Hon. Bernard Fried*	Hon. Judith Gische
Hon. Teresa Johnson	Hon. Barry Kamins*	Hon. John Leventhal
Hon. Martin Marcus	Hon. Robert Miller	Hon. Mary Work*

* Retired