Part One

ADMISSIBILITY OF COMPUTERIZED RECORDS

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.

II. FOUNDATION

A. 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]).

B. 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]).

C. 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]).

III. Medical Records

A. Generally

1. 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/).

2. 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]).

3. 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).

4. 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).

B. Audit Trail

1. 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).

2. 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).

3. 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. For further discussion, *see* Blind, The Electronic Health Record: A Discovery and Production Nightmare, 58 Univ Louisville L. Rev. 303 (2018).

Part Two

ADMISSIBILITY OF E-MAILS AND SOCIAL MEDIA POSTS

I. 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]).

(a) 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]).

(b) 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])

(c) 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"]).

1. 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).

(d) 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]).

(e) 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).

1. 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]).

II. SOCIAL MEDIA POSTS

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 *420 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.

Part Three

ATTORNEY 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. ATTORNEY CLIENT PRIVILEGE

A. Waiver

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)."

(c) 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]).