

## Appendix A (100114mins)



**SELECTED MATERIALS ON EVIDENTIARY ISSUES  
RELATING TO ELECTRONICALLY STORED INFORMATION**

Prepared for Code of Evidence Oversight Committee  
by Judge Steven D. Ecker  
October 1, 2014



## TABLE OF CONTENTS

1. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. 2011) . . . . .
2. State v. Swinton, 268 Conn. 781 (2004) (excerpts) . . . . .
3. State v. Elleck, 130 Conn. App. 632 (2011) (Bishop, J.) . . . . .
4. Federal Rules of Evidence 101, 104, 901, 902 . . . . .
5. Preliminary Selected Bibliography . . . . .



241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

▷

United States District Court,  
D. Maryland.  
Jack R. LORRAINE and, Beverly Mack, Plaintiffs,  
v.  
MARKEL AMERICAN INSURANCE COMPANY,  
Defendants.

Civil Action No. PWG-06-1893.  
May 4, 2007.

**Background:** Suit was brought to enforce arbitrator's award. Parties moved and cross moved for summary judgment.

**Holding:** The District Court, Grimm, Chief United States Magistrate Judge, held that failure of both parties to observe evidence rules, as they applied to electronically stored information (ESI), precluded any entry of summary judgment.

Motions denied.

West Headnotes

[1] **Alternative Dispute Resolution 25T** ⚡ **200**

25T Alternative Dispute Resolution  
25TII Arbitration  
25TII(D) Performance, Breach, Enforcement,  
and Contest  
25Tk197 Matters to Be Determined by  
Court  
25Tk200 k. Arbitrability of Dispute.  
Most Cited Cases

When the parties to an arbitration agreement do

not agree to submit questions of arbitrability to the arbitrator for resolution, determining the scope of the agreement is an issue for the court to decide.

[2] **Evidence 157** ⚡ **351**

157 Evidence  
157X Documentary Evidence  
157X(C) Private Writings and Publications  
157k351 k. Unofficial or Business Records  
in General. Most Cited Cases

In order for electronically stored information (ESI) to be admissible, it must be (1) relevant, (2) authentic, (3) not hearsay or admissible under an exception to rule barring hearsay evidence, (4) original or duplicate, or admissible as secondary evidence to prove its contents, and (5) probative value must outweigh its prejudicial effect. Fed.Rules Evid.Rules 401, 403, 803, 804, 807, 901(a), 1001-1008, 28 U.S.C.A.

[3] **Federal Civil Procedure 170A** ⚡ **2545**

170A Federal Civil Procedure  
170AXVII Judgment  
170AXVII(C) Summary Judgment  
170AXVII(C)3 Proceedings  
170Ak2542 Evidence  
170Ak2545 k. Admissibility. Most  
Cited Cases

Failure of counsel for both sides, in suit to compel arbitration, to observe evidence rules concerning electronically stored information (ESI), particularly rules governing authenticity, hearsay issues, original writing rule, and absence of unfair prejudice, rendered their summary judgment exhibits inadmissible. Fed.Rules Evid.Rules 401, 403, 803, 804, 807, 901(a), 1001-1008, 28 U.S.C.A.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

\*534 Geoffrey S. Tobias, Ober Kaler Grimes and Shriver, Baltimore, MD, for Plaintiffs.

Peter Joseph Basile, Ferguson Schetelich and Ballew PA, Baltimore, MD, for Defendant.

#### MEMORANDUM OPINION

GRIMM, Chief United States Magistrate Judge.

Plaintiffs/Counter-Defendants Jack Lorraine and Beverly Mack bring this action to enforce a private arbitrator's award finding that certain damage to their yacht, *Chessie*, was caused by a lightning strike that occurred on May 17, 2004, while *Chessie* was anchored in the Chesapeake Bay.<sup>FN1</sup> Defendant/ Counter-Plaintiff Markel American Insurance Company ("Markel") likewise has counterclaimed to enforce the arbitrator's award, which, in addition to concluding that certain damage to *Chessie's* hull was caused by lightning, also concluded that the damage incurred was limited to an amount of \$14,100, plus incidental costs. Following discovery, Plaintiffs moved for summary judgment (Paper No. 16), and Defendants filed a response in opposition and cross motion for summary judgment (Paper No. 19), to which Plaintiffs filed an opposition and reply (Paper No. 21), followed by Defendant's reply (Paper No. 23). In a letter order dated February 7, 2007 (Paper No. 26), I denied without prejudice both motions for the reasons discussed more fully below, and informed the parties that I intended to file a more comprehensive opinion explaining my ruling, which is found herein.

FN1. This case has been referred to me for all proceedings with the consent of the parties. 28 U.S.C. § 636(c)(1)(2006); Local Rule 301.4.

#### BACKGROUND

It is difficult for the Court to provide the appropriate background to the underlying \*535 arbitration in this case because, as will be discussed in greater

detail below, neither party has proffered any admissible evidence to support the facts set forth in their respective motions. See FED.R.CIV.P. 56(c). Based on the pleadings, however, it appears undisputed that *Chessie* was struck by lightning on May 17, 2004, and that Plaintiffs filed a claim with Markel, their insurance carrier, for certain damage incurred as a result of the strike. Compl. ¶¶ 5, 6; Answer ¶¶ 2, 6. Markel issued payment under the policy for some of the damage claimed, and the matter would have been concluded had Plaintiffs not discovered damage to the hull when they pulled the boat out of the water several months later. Compl. ¶ 7. Markel denied that the hull damage was caused by the lightning strike and/or covered by Plaintiffs' insurance policy, and initiated a declaratory judgment action in the United States District Court for the Middle District of Pennsylvania to that effect. Compl. ¶ 13, Answer ¶ 15. The parties subsequently negotiated a private arbitration agreement and voluntarily dismissed the Pennsylvania claim. Compl. ¶ 15, Answer ¶ 17.

The scope of the arbitration agreement is the basis of this litigation. The final agreement states, in relevant part,

"The parties to this dispute ... have agreed that an arbitrator shall determine whether certain bottom damage in the amount of \$36,000, to the Yacht CHESSIE was caused by the lightning strike occurring on May 17, 2004, or osmosis, as claimed by [Markel]."

Pl.'s Mot. Ex. A, Def.'s Mot. Ex. C. The agreement also contemplated that the arbitrator would issue an "award" within 30 days of the final submission of evidence. *Id.* The arbitrator issued his award on June 12, 2006. In it, he held that some, but not all, of *Chessie's* hull damage was caused by lightning. Specifically, the arbitrator stated,

"I find that there is a basis for an argument regarding loss related damage. Evidence shows that the lightning strike on Mary 17, 2004 was discharged

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

through the hull below the water line.... The **corruption** of the surface laminate of the bottom is basis for a loss related award.... The award amount must be kept in proportion to the **loss related damage** only. I find that the repairs relating to that damage should be based on a cost of \$300.00 per foot (\$14,000.00). Other expenses relating to charges for hauling, mast un-stepping/re-stepping, blocking, storage, moving, launching or environmental fees should be added to that amount.”

Def.'s Mot. Ex. D. This award forms the basis for the present litigation, in which both parties ostensibly seek to confirm and enforce the arbitrator's decision.

#### SUMMARY JUDGMENT STANDARD

Summary judgment is appropriate when there exists no genuine issue as to any material fact and a decision may be rendered as a matter of law. Fed.R.Civ.P. 56(c); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). The party moving for summary judgment has the burden of demonstrating that there are no genuine issues of material facts to resolve. *Pulliam Inv. Co. v. Cameo Properties*, 810 F.2d 1282, 1286 (4th Cir.1987). In determining whether summary judgment should be granted, the court “must assess the documentary materials submitted by the parties in the light most favorable to the nonmoving party.” *Id.* (citing *Gill v. Rollins Protective Services Co.*, 773 F.2d 592, 598 (4th Cir.1985)).

If the party seeking summary judgment demonstrates that there is no evidence to support the non-moving party's case, the burden shifts to the non-moving party to identify specific facts showing that there is a genuine issue for trial. The existence of only a “scintilla of evidence” is not enough to defeat a motion for summary judgment. Instead, the evidentiary materials submitted must show facts from which the finder of fact reasonably could find for the party opposing summary judgment. *Anderson*, 477 U.S. at 251, 106 S.Ct. 2505.

Moreover, 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 FED.R.CIV.P. 56(c); see also *Sakaria v. Trans World Airlines*, 8 F.3d 164, 171 (4th Cir.1993) (finding that the district court \*536 properly did not consider inadmissible hearsay in an affidavit filed with motion for summary judgment); *Mitchell v. Data General Corp.*, 12 F.3d 1310, 1315-16 (4th Cir.1993) (“The summary judgment inquiry thus scrutinizes the plaintiff's case to determine whether the plaintiff has proffered sufficient proof in the form of admissible evidence that could carry the burden of proof in his claim at trial.”). 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.”

*Miskin v. Baxter Healthcare Corp. et al.*, 107 F.Supp.2d 669 (D.Md.1999) (Grimm, J.) (citing *Orsi v. Kirkwood*, 999 F.2d 86, 92 (4th Cir.1993)).

#### THE FEDERAL ARBITRATION ACT

As a preliminary matter, Plaintiffs have styled their complaint as one to enforce the arbitrator's award under § 9 of the Federal Arbitration Act, 9 U.S.C. § 1 et seq. (2006), when, in reality, it is a complaint to *modify* the award under section 10 of that statute. This is so because, although the arbitrator found that only \$14,100 of *Chessie's* hull damage was caused by lightning, Plaintiffs nonetheless ask the Court to award a judgment in the amount of \$36,000. Plaintiffs' argument regarding the substance of the agreement between the parties further underscores this conclu-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

sion. Specifically, Plaintiffs allege that the parties entered into an “all or nothing” agreement, whereby the arbitrator was to determine that the hull damage was caused by lightning, and if so, award Plaintiffs the \$36,000.00 in damages claimed. Pl.’s MSJ at 5. According to Plaintiffs,

“the Arbitrator’s sole function was to determine whether the hull damage, in the agreed-upon amount of \$36,000, was caused by the lightning strike occurring on May 17, 2004. *The Arbitration Agreement did not grant the Arbitrator the authority to assess a damage amount.*”

*Id.* (emphasis added). This argument is consistent with a motion to modify under § 10(b)(4), which permits a federal court to modify or vacate an arbitration award upon a showing that “the arbitrator[ ] exceeded their powers.” Accordingly, the Court will evaluate Plaintiffs’ motion under § 10 of the FAA.

In contrast, Markel’s complaint truly is one to enforce the arbitrator’s award. Markel denies that it entered into an “all or nothing” arbitration agreement with regard to damages, and seeks to enforce the arbitrator’s award of \$14,100. Def.’s Mot. at 5.

The question before the Court, therefore, is whether the arbitrator exceeded his authority under the arbitration agreement by assigning a value to the damages attributable to the lightning strike that was less than the \$36,000 claimed by Plaintiffs. If the answer is yes, then the court can vacate, remand, or modify the award. 9 U.S.C. § 10, 11. If the answer is no, then the court must grant Defendant’s motion to confirm the award under § 9 of the FAA.

[1] To resolve whether the arbitrator exceeded his authority, the Court first must determine the scope of the arbitration agreement; specifically, whether the parties agreed to arbitrate the amount of damages caused by the lightning strike. Because the parties did

not agree to submit questions of arbitrability to the arbitrator for resolution, determining the scope of the agreement is an issue for the Court to decide. *First Options of Chicago, Inc. v. Kaplan*, 514 U.S. 938, 943, 115 S.Ct. 1920, 131 L.Ed.2d 985 (1995). In this regard, the Supreme Court has advised that, “[w]hen deciding whether the parties agreed to arbitrate a certain matter ... courts generally ... should apply ordinary state-law principles of contract interpretation.” *Kaplan*, 514 U.S. at 944, 115 S.Ct. 1920, *accord E.I. DuPont De Nemours & Co. v. Martinsville Nylon Employees’ Council Corp.*, 78 F.3d 578 (4th Cir.1996). In doing so, the Court must “give due regard to the federal policy favoring arbitration and resolve ‘any doubts concerning the scope of arbitrable issues in favor of arbitration.’ ” *Hill v. PeopleSoft USA, Inc.*, 412 F.3d 540, 543 (4th Cir.2005) (quoting \*537 *Moses H. Cone Mem’l Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 24-25, 103 S.Ct. 927, 74 L.Ed.2d 765 (1983)). Maryland law <sup>FN2</sup> regarding contract interpretation requires the court first to “determine from the language of the agreement itself what a reasonable person in the position of the parties would have meant at the time it was effectuated.” *GMAC v. Daniels*, 303 Md. 254, 262, 492 A.2d 1306, 1310 (Md.1985). If the language of the contract is clear and unambiguous, then the Court “must presume that the parties meant what they expressed.” *Id.* If the language of the contract is ambiguous, however, the court may consider parol evidence to determine the intent of the parties. *E.g. Truck Ins. Exch. v. Marks Rentals, Inc.*, 288 Md. 428, 433, 418 A.2d 1187, 1190 (Md.1980). Contract language is ambiguous if it could be read to have more than one meaning by a reasonably prudent layperson. *Clendenin Bros., Inc. v. United States Fire Ins. Co.*, 390 Md. 449, 459, 889 A.2d 387, 393-394 (Md.2006), citing *Truck Ins. Exch.*, 288 Md. at 433, 418 A.2d at 1190.

FN2. The parties do not dispute that Maryland law applies.

Here, I find that the language of the arbitration

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

agreement is ambiguous; it could be read either to permit the arbitrator to determine the amount of damage to *Chessie*, or to limit his authority to determining only whether the claimed damages were caused by the lightning strike. Under normal circumstances, the Court would look to the documentary evidence provided by the parties, which in this case includes the arbitration agreement, award, and copies of e-mail correspondence between counsel, ostensibly supplied as extrinsic evidence of the parties' intent with regard to the scope of the arbitration agreement. In this case, however, the admissibility problems with the evidence presented are manifest. First, none of the documentary evidence presented is authenticated by affidavit or otherwise. Next, most of the facts relevant to the contract negotiations at issue have been provided by counsel *ipse dixit*, without supporting affidavits or deposition testimony. The evidentiary problems associated with the copies of e-mail offered as parol evidence likewise are substantial because they were not authenticated, but instead were simply attached to the parties' motions as exhibits.

Because neither party to this dispute complied with the requirements of Rule 56 that they support their motions with admissible evidence, I dismissed both motions without prejudice to allow resubmission with proper evidentiary support. (Paper No. 26). I further observed that the unauthenticated e-mails are a form of computer generated evidence that pose evidentiary issues that are highlighted by their electronic medium. Given the pervasiveness today of electronically prepared and stored records, as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence. Although cases abound regarding the discoverability of electronic records, research has failed to locate a comprehensive analysis of the many interrelated evidentiary issues associated with electronic evidence. Because there is a need for guidance to the bar regarding this subject, this opinion undertakes a broader

and more detailed analysis of these issues than would be required simply to resolve the specific issues presented in this case. It is my hope that it will provide a helpful starting place for understanding the challenges associated with the admissibility of electronic evidence.

#### ADMISSIBILITY OF ELECTRONICALLY STORED INFORMATION

Be careful what you ask for, the saying goes, because you might actually get it. For the last several years there has been seemingly endless discussion of the rules regarding the discovery of electronically stored information ("ESI"). The adoption of a series of amendments to the Federal Rules of Civil Procedure relating to the discovery of ESI in December of 2006 has only heightened, not lessened, this discussion. Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes "such facts as would \*538 be admissible in evidence" for use in summary judgment practice. FED.R.CIV.P. 56(e).<sup>FN3</sup> This is unfortunate, because considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted. The process is complicated by the fact that ESI comes in multiple evidentiary "flavors," including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files.<sup>FN4</sup>

FN3. See, e.g. *Orsi v. Kirkwood*, 999 F.2d 86, 92 (4th Cir.1993) ("It is well established that unsworn, unauthenticated documents cannot be considered on a motion for summary judgment"); *Planmatics, Inc. v. Showers*, 137 F.Supp.2d 616, 620 (D.Md.2001) ("On a motion for summary judgment, a district court may only consider evidence that would

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

be admissible at trial” (citations omitted)). See also *Maryland Highways Contractors Assoc., Inc. v. State of Maryland*, 933 F.2d 1246, 1251 (4th Cir.1991); *Wilson v. Clancy*, 747 F.Supp. 1154, 1158 (D.Md.1990); JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.02 [1] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997)(hereinafter “WEINSTEIN”).

FN4. Examples of internet postings include; data posted by the site owner, data posted by others with the consent of the site owner, and data posted by others without consent, such as “hackers.” Examples of computer-generated documents and files include; electronically stored records or data, computer simulation, and computer animation. See 2 MCCORMICK ON EVIDENCE § 227 (John William Strong, et al. eds., 6th ed.2006); Gregory P. Joseph, *Internet and Email Evidence*, 13 PRAC. LITIGATOR (Mar.2002), reprinted in 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL, Part 4 at 20 (9th ed.2006)(hereinafter “Joseph”); Hon. Paul W. Grimm and Claudia Diamond, *Low-Tech Solutions to High-Tech Wizardry: Computer Generated Evidence*, 37 MD. B.J. 4 (July/August, 2004).

[2] Whether ESI is admissible into evidence is determined by a collection of evidence rules<sup>FNS</sup> 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 prob-

able 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, of 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. Preliminarily, the process by which the admissibility of ESI is determined is governed by Rule 104, which addresses the relationship between the judge and the jury with regard to preliminary fact finding associated with the admissibility of evidence. Because Rule 104 governs the very process of determining admissibility of ESI, it must be considered first.

FN5. It has been noted that “[t]he Federal Rules of Evidence ... do not separately address the admissibility of electronic data.” ADAM COHEN AND DAVID LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE § 6.01 (Aspen Publishers 2007). However, “the Federal Rules of Evidence apply to computerized data as they do to other types of evidence.” MANUAL FOR COMPLEX LITIGATION § 11.447 (4th ed.2004). Indeed, FED.R.EVID. 102 contemplates that the rules of evidence are flexible enough to accommodate future “growth and development” to address technical changes not in existence as of the codification of the rules themselves. Further, courts have had little difficulty using the existing rules of evidence to determine the admissibility of ESI, despite the technical challenges that sometimes must be overcome

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

to do so. *See, e.g., In re F.P.*, 878 A.2d 91, 95 (Pa.Super.Ct.2005) (“Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages.... We believe that e-mail messages and similar forms of electronic communications can be properly authenticated within the existing framework of [the state rules of evidence].”).

**\*539 Preliminary Rulings on Admissibility(Rule 104)**

The relationship between Rule 104(a) and (b) can complicate the process by which ESI is admitted into evidence at trial, or may be considered at summary judgment. The rule states, in relevant part:

“(a) Questions of admissibility generally. Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b).... In making its determination it is not bound by the rules of evidence except those with respect to privileges.

(b) Relevancy conditioned on fact. When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.”

FED.R.EVID. 104(a) and (b).

When the judge makes a preliminary determination regarding the admissibility of evidence under Rule 104(a), the Federal Rules of Evidence, except for privilege, do not apply. Rule 104(a), 1101(d)(1). Therefore, the court may consider hearsay or other evidence that would not be admissible if offered to the jury,<sup>FN6</sup> and “hearings on preliminary matters need not

be conducted with all the formalities and requirements of a trial.”<sup>FN7</sup> Accordingly, the trial judge may make preliminary determinations in chambers or at a sidebar conference in court.<sup>FN8</sup>

FN6. *Precision Piping and Instruments v. E.I. du Pont de Nemours and Co.*, 951 F.2d 613, 621 (4th Cir.1991); 1 STEPHEN A. SALTZBURG ET AL., *FEDERAL RULES OF EVIDENCE MANUAL*, 104.03[1][b] (9th ed.2006)(hereinafter “SALTZBURG”); WEINSTEIN at § 104.11[1][a]; *Id.* at § 901.06[1][c][iii] (“Rule 104(a) provides that inadmissible evidence may be considered in determining preliminary questions of admissibility under Rule 104(a). However, that provision does not extend to determinations under Rule 104(b), so the court may not consider inadmissible evidence in determinations governed by Rule 104(b). In determining the preliminary question of authenticity under Rule 104(b), therefore, a judge may only consider evidence that is itself admissible.”).

FN7. WEINSTEIN at § 104.11[3].

FN8. *Id.*; *United States v. Branch*, 970 F.2d 1368 (4th Cir.1992).

The following types of preliminary matters typically are determined by the judge under Rule 104(a): whether an expert is qualified, and if so, whether his or her opinions are admissible; existence of a privilege; and whether evidence is hearsay, and if so, if any recognized exception applies.<sup>FN9</sup>

FN9. WEINSTEIN at § 104.02[2].

The interplay between Rule 104(a) and 104(b) can be a bit tricky, which is illustrated by the manner in which evidence, whether ESI or “hard copy,” must

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

be authenticated under Rule 901(a). Authentication under Rule 901 is viewed as a subset of relevancy, because “evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims.”<sup>FN10</sup> Accordingly, “[r]esolution of whether evidence is authentic calls for a factual determination by the jury and admissibility, therefore, is governed by the procedure set forth in Federal Rule of Evidence 104(b) ‘relating to matters of conditional relevance generally.’ ”<sup>FN11</sup> In essence, determining whether ESI is authentic, and therefore relevant, is a two step process. First, “[b]efore admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic.”<sup>FN12</sup> Then, “because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which \*540 the proponent claims.”<sup>FN13</sup> As the Fourth Circuit summarized this process:

FN10. *Branch*, 970 F.2d at 1370 (citing *United States v. Sliker*, 751 F.2d 477, 497-99 (2d Cir.1984)).

FN11. *Id.* (citation omitted). *See also*, FED.R.EVID. 901(a) advisory committee’s notes (“Authentication and identification represent a special aspect of relevancy.... This requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b)”).

FN12. *Branch*, 970 F.2d at 1370 (citing FED.R.EVID. 104(b) advisory committee’s note).

FN13. *Id.* at 1370-71.

“Although the district court is charged with making this preliminary determination, because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims. Because the ultimate resolution of authenticity is a question for the jury, in rendering its preliminary decision on whether the proponent of evidence has laid a sufficient foundation for admission the district court must necessarily assess the adequacy of the showing made before the jury.”<sup>FN14</sup>

FN14. *Id.* (citation omitted)

With respect to this two step process, the Fourth Circuit went on to state:

“[a]n in camera hearing addressing authenticity does not replace the presentation of authenticating evidence before the jury; the district court must revisit this issue at trial. Thus, even though the district court may have ruled during an in camera proceeding that the proponent had presented sufficient evidence to support a finding that [the evidence] was authentic, evidence that would support the same ruling must be presented again, to the jury, before the [evidence] may be admitted.”<sup>FN15</sup>

FN15. *Id.*

In short, there is a significant difference between the way that Rule 104(a) and 104(b) operate. Because, under Rule 104(b), the jury, not the court, makes the factual findings that determine admissibility, the facts introduced must be admissible under the rules of evidence.<sup>FN16</sup> It is important to understand this relationship when seeking to admit ESI. For example, if an e-mail is offered into evidence, the determination of whether it is authentic would be for the jury to decide under Rule 104(b), and the facts that they

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

consider in making this determination must be admissible into evidence. In contrast, if the ruling on whether the e-mail is an admission by a party opponent or a business record turns on contested facts, the admissibility of those facts will be determined by the judge under 104(a), and the Federal Rules of Evidence, except for privilege, are inapplicable.

FN16. See, e.g., *United States v. Safavian*, 435 F.Supp.2d 36, 41-42 (D.D.C.2006) (trial judge relied on proffers of government lawyers about facts learned by FBI agents during their investigation to make preliminary determination that e-mails were admissible, but cautioned that at trial the government would have to call witnesses with personal knowledge of facts and not rely on FBI agents' testimony about what others had told them regarding the origin of the e-mails); SALTZBURG at § 901.02[5] ("In order for the trier of fact to make a rational decision as to authenticity [under Rule 104(b)], the foundation evidence must be admissible and it must actually be placed before the jury if the Judge admits the evidence").

#### **Relevance (Rules 401, 402, and 105)**

The first evidentiary hurdle to overcome in establishing the admissibility of ESI is to demonstrate that it is relevant, as defined by Federal Rule of Evidence 401, which states:

" 'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."

Clearly, facts that tend to prove essential elements of the causes of action and affirmative defenses asserted in the pleadings are "of consequence to the litigation," as are facts that tend to undermine or re-

habilitate the credibility of the witnesses who will testify. SALTZBURG at § 401.02[8]. So too, however, are background facts that, although they may not prove elements of the claims and defenses, and may not even be disputed, nonetheless routinely are admitted to help the fact finder understand the issues in the case and the evidence introduced to prove or disprove them. FED.R.EVID. 401 advisory committee's note. It is important to recognize that relevance is not a static concept; evidence is not relevant or irrelevant, occupying some rigid state of all or nothing. SALTZBURG at § 401.02[11]. Instead, "[r]elevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter \*541 properly provable in the case." FED.R.EVID. 401 advisory committee's note. As recognized by Federal Rule of Evidence 105, evidence may be admissible for one purpose, but not another, or against one party, but not another.<sup>FN17</sup> Therefore, it is important for the proponent of the evidence to have considered all of the potential purposes for which it is offered, and to be prepared to articulate them to the court if the evidence is challenged. This point is particularly significant, as discussed below, when considering hearsay objections, where disputed evidence may be inadmissible hearsay if offered for its substantive truth, but admissible if offered for a reason other than its literal truth.

FN17. FED R. EVID. 105 states: "When evidence which is admissible as to one party or for one purpose but not admissible as to another party or for another purpose is admitted, the court, upon request, shall restrict the evidence to its proper scope and instruct the jury accordingly."

In assessing whether evidence is relevant under Rule 401, it also is important to remember that there is a distinction between the admissibility of evidence, and the weight to which it is entitled in the eyes of the fact finder, as Rule 104(e) <sup>FN18</sup> instructs. To be relevant, evidence does not have to carry any particular

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

weight-it is sufficient if it has "any tendency" to prove or disprove a consequential fact in the litigation. Whether evidence tends to make a consequential fact more probable than it would be without the evidence is not a difficult showing to make. FED.R.EVID. 401 advisory committee's note; SALTZBURG at § 401.02[1] ("To be relevant it is enough that the evidence has a *tendency* to make a consequential fact even the least bit more probable or less probable than it would be without the evidence. The question of relevance is thus different from whether evidence is *sufficient* to prove a point.") See also WEINSTEIN at § 401.05-06.

FN18. FED.R.EVID. 104(e) states: "[Rule 104] does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility [of evidence that has been admitted by an adverse party]."

The Federal Rules of Evidence are clear: evidence that is not relevant is never admissible. FED.R.EVID. 402. Once evidence has been shown to meet the low threshold of relevance, however, it presumptively is admissible unless the constitution, a statute, rule of evidence or procedure, or case law requires that it be excluded.<sup>FN19</sup> Thus, the function of all the rules of evidence other than Rule 401 is to help determine whether evidence which in fact is relevant should nonetheless be excluded. FED.R.EVID. 402 advisory committee's note ("Succeeding rules [in Article IV of the rules of evidence] ... in response to the demands of particular policies, require the exclusion of evidence despite its relevancy."). See also SALTZBURG § 402.02 [1]-[2].

FN19. *Id.* (stating that "[a]ll relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissi-

ble."); SALTZBURG at § 401.02[1]; WEINSTEIN at § 402.02[1].

Establishing that ESI has some relevance generally is not hard for counsel. Articulating all of what may be multiple grounds of relevance is something that is important, though not as frequently done as it should be. Accordingly, evidence that might otherwise be admitted may be excluded because the proponent put all his or her eggs in a single evidentiary basket, which the trial judge views as inapplicable, instead of carefully identifying each potential basis for admissibility. That was not the problem in this case, however, because the e-mail and other documentary evidence attached as exhibits to the summary judgment motions are relevant to determining the scope of the arbitration agreement between the parties, and therefore this evidence meets the requirements of Rule 401. Assuming, as is the case here, the proponent of ESI establishes its relevance and concomitant presumptive admissibility, the next step is to demonstrate that it is authentic. It is this latter step that the parties in this case omitted completely.

#### *Authenticity (Rules 901-902)*

In order for ESI to be admissible, it also must be shown to be authentic. Rule 901(a) defines what this entails: "[t]he requirement \*542 of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." As already noted, "[a]uthentication and identification represent a special aspect of relevancy.... 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 Rule 104(b)." FED.R.EVID. 901 advisory committee's note. The requirement of authentication and identification also insures that evidence is trustworthy, which is especially important in analyzing hearsay issues. Indeed, these two evidentiary concepts often are considered together when determining the admissibility of ex-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

hibits or documents.<sup>FN20</sup> WEINSTEIN at § 901.02[2].

FN20. *See, e.g., In re Vee Vinhnee*, 336 B.R. 437, 444 (9th Cir. BAP 2005) (In considering admissibility of electronically stored business records, the court noted “[o]rdinarily, because the business record foundation commonly covers the ground, the authenticity analysis [under Rule 902(11)] is merged into the business record analysis without formal focus on the question.” (citation omitted)).

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. *Id.* at § 901.02[3]. This is not a particularly high barrier to overcome. For example, in *United States v. Safavian*, the court analyzed the admissibility of e-mail, noting,

“[t]he question for the court under Rule 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.”

435 F.Supp.2d at 38 (citations omitted). *See also United States v. Meienberg*, 263 F.3d 1177, 1180 (10th Cir.2001) (analyzing admissibility of printouts of computerized records); *United States v. Tank*, 200 F.3d 627, 630 (9th Cir.2000) (analyzing admissibility of exhibits reflecting chat room conversations); *United States v. Reilly*, 33 F.3d 1396, 1404 (3d Cir.1994)(discussing admissibility of radiotelegrams); *United States v. Howard-Arias*, 679 F.2d 363, 366 (4th Cir.1982)(addressing chain of authenticity); *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at \* 16 (N.D.Ill. Oct.15, 2004) (analyzing admissibility of the content of a

website).

Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation. *See, e.g., In re Vee Vinhnee*, 336 B.R. 437 (proponent failed properly to authenticate exhibits of electronically stored business records); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir.2000) (proponent failed to authenticate exhibits taken from an organization's website); *St. Luke's Cataract and Laser Institute PA v. Sanderson*, 2006 WL 1320242, at \*3-4 (M.D.Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Rambus v. Infineon Tech. AG*, 348 F.Supp.2d 698 (E.D.Va.2004) (proponent failed to authenticate computer generated business records); *Wady v. Provident Life and Accident Ins. Co. of Am.*, 216 F.Supp.2d 1060 (C.D.Cal.2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Assoc., Inc. v. Wiley*, 1998 WL 1988826, at \*7 (S.D.Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them).

Although courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication\*543 of “hard copy” documents,<sup>FN21</sup> they have been quick to reject calls to abandon the existing rules of evidence when doing so. For example, in *In re F.P.* the court addressed the authentication required to introduce transcripts of instant message conversations. In rejecting the defendant's challenge to this evidence, it stated:

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

FN21. In *In re Vee Vinhnee*, the court addressed the authentication of electronically stored business records. It observed “[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained....” However, it quickly noted “[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records. Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be.” The court did conclude, however, that “it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground,” before exercising a demanding analysis of the foundation needed to authenticate a paperless business record and lay the foundation for the business record exception to the hearsay rule, ultimately ruling that a proper foundation had not been established, and excluding the evidence. 336 B.R. at 444-45. *See also* MANUAL FOR COMPLEX LITIGATION at § 11.447 (“In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, 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. The

judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pre-trial proceedings, so that challenges to the evidence are not made for the first time at trial.”).

“Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationery can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa.R.E. 901 and Pennsylvania case law ... We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.”

878 A.2d at 95-96. Indeed, 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. As one respected commentator on the Federal Rules of Evidence has noted:

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

"In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.

\*544 The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination. Factors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems. The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer processing.

Determining what degree of foundation is appropriate in any given case is in the judgment of the court. The required foundation will vary not only with the particular circumstances but also with the individual judge."

WEINSTEIN at § 900.06[3]. Obviously, there is no "one size fits all" approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges.

Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished. It states:

"(b) Illustrations.

By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

(1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.

(2) Nonexpert opinion on handwriting. Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.

(3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.

(4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

(5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.

(6) Telephone conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

(7) Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(8) Ancient documents or data compilation. Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) Methods provided by statute or rule. Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority."

The ten methods identified by Rule 901(b) are non-exclusive. FED.R.EVID. 901(b) 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."); WEIN\*545 STEIN at § 901.03[1] ("Parties may use any of the methods listed in Rule 901(b), 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."); *Telewizja Polska USA*, 2004 WL 2367740 (authentication methods listed in Rule 901(b) are "non-exhaustive"). See also *United States v. Simpson*, 152 F.3d 1241, 1249 (10th Cir.1998) (evaluating methods of authenticating a printout of the text of a chat room discussion between the defendant and an undercover detective in a child pornography case).

Although the methods of authentication listed in Rule 901(b) "relate for the most part to documents ... some attention [has been] given to ... computer print-outs," particularly Rule 901(b)(9), which was drafted with "recent developments" in computer technology in mind. FED.R.EVID. 901(b) advisory committee's note. When faced with resolving authentication issues for electronic evidence, courts have used a number of the methods discussed in Rule 901(b), as well as approved some methods not included in that rule:

#### *Rule 901(b)(1).*

This rule permits authentication by: "[t]estimony that a matter is what it is claimed to be." This rule "contemplates a broad spectrum" including "testimony of a witness who was present at the signing of a document...." FED.R.EVID. 901(a) advisory committee's note. "[I]n recognition of the proponent's light burden of proof in authenticating an exhibit ... the 'knowledge' requirement of Rule 901(b)(1) is liberally construed. A witness may be appropriately knowledgeable through having participated in or observed the event reflected by the exhibit." WEINSTEIN at § 901.03[2] (cross-reference omitted). Courts considering the admissibility of electronic evidence frequently have acknowledged that it may be authenticated by a witness with personal knowledge. *United States v. Kassimu*, 2006 WL 1880335 (5th Cir. May 12, 2006) (ruling that copies of a post office's computer records could be authenticated by a custodian or other qualified witness with personal knowledge of the procedure that generated the rec-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

ords); *St. Luke's*, 2006 WL 1320242 at \*3-4 (“To authenticate printouts from a website, the party proffering the evidence must produce ‘some statement or affidavit from someone with knowledge [of the website] ... for example [a] web master or someone else with personal knowledge would be sufficient.’ ” (citation omitted)); *Safavian*, 435 F.Supp.2d at 40 n. 2 (D.D.C.2006) (noting that e-mail may be authenticated by a witness with knowledge that the exhibit is what it is claimed to be); *Wady*, 216 F.Supp.2d 1060 (sustaining objection to affidavit of plaintiff’s witness attempting to authenticate documents taken from the defendant’s website because the affiant lacked personal knowledge of who maintained the website or authored the documents). Although Rule 901(b)(1) certainly is met by the testimony of a witness that actually drafted the exhibit, it is not required that the authenticating witness have personal knowledge of the making of a particular exhibit if he or she has personal knowledge of how that type of exhibit is routinely made. WEINSTEIN at § 901.03[2].<sup>FN22</sup> It is necessary, however, that the authenticating witness provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business record\*546 exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8).

FN22. “Oftentimes a witness need not be familiar with specific exhibits to be sufficiently knowledgeable to authenticate or identify them. Business records and records of government agencies, for example, are frequently authenticated by witnesses who have never seen the specific records that comprise the exhibits and know nothing about the specific information they contain. Their authentication is accomplished when a witness identifies the exhibits as documents

of a type that the organization typically develops, and testifies about the procedures the organization follows in generating, acquiring, and maintaining documents of that type, and explains the method by which the specific exhibits were retrieved from the organization’s files. Similarly, exhibits that are automatically produced upon the occurrence of specified events may be authenticated by the testimony of persons with knowledge of the system or process that results in the production of the exhibit.” (footnote omitted).

#### **Rule 901(b)(3).**

This rule allows authentication or identification by “[c]omparison by the trier of fact or by expert witnesses with specimens which have been authenticated.” Interestingly, the rule allows either expert opinion testimony to authenticate a questioned document by comparing it to one known to be authentic, or by permitting the factfinder to do so. Obviously, the specimen used for the comparison with the document to be authenticated must be shown itself to be authentic. WEINSTEIN at § 901.03[7][b]. This may be accomplished by any means allowable by Rule 901 or 902, as well as by using other exhibits already admitted into evidence at trial, or admitted into evidence by judicial notice under Rule 201. *Id.* Although the common law origin of Rule 901(b)(3) involved its use for authenticating handwriting or signatures, FED. R. EVID. 901(b)(3) advisory committee’s note, it now is commonly used to authenticate documents, WEINSTEIN at § 901.03[7][b], and at least one court has noted its appropriate use for authenticating e-mail. *Safavian*, 435 F.Supp.2d at 40 (E-mail messages “that are not clearly identifiable on their own can be authenticated ... by comparison by the trier of fact (the jury) with ‘specimens which have been [otherwise] authenticated’-in this case, those e-mails that already have been independently authenticated under Rule 901(b)(4).”).

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

**Rule 901(b)(4.)**

This rule is one of the most frequently used to authenticate e-mail and other electronic records. It permits exhibits to be authenticated or identified by “[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.” The commentary to Rule 901(b)(4) observes “[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety,” including authenticating an exhibit by showing that it came from a “particular person by virtue of its disclosing knowledge of facts known peculiarly to him,” or authenticating “by content and circumstances indicating it was in reply to a duly authenticated” document. FED.R.EVID. 901(b)(4) advisory committee’s note. Use of this rule often is characterized as authentication solely by “circumstantial evidence.” WEINSTEIN at § 901.03[8]. Courts have recognized this rule as a means to authenticate ESI, including e-mail, text messages and the content of websites. *See United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir.2000) (allowing the authentication of an e-mail entirely by circumstantial evidence, including the presence of the defendant’s work e-mail address, content of which the defendant was familiar with, use of the defendant’s nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the e-mail); *Safavian*, 435 F.Supp.2d at 40 (same result regarding e-mail); *In re F.P.*, 878 A.2d at 94 (noting that authentication could be accomplished by direct evidence, circumstantial evidence, or both, but ultimately holding that transcripts of instant messaging conversation circumstantially were authenticated based on presence of defendant’s screen name, use of defendant’s first name, and content of threatening message, which other witnesses had corroborated); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146, 1153-54 (C.D.Cal.2002) (admitting website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses).

One method of authenticating electronic evidence under Rule 901(b)(4) is the use of “hash values” or “hash marks” when making documents. A hash value is:

“A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. ‘Hashing’ is used to guarantee the authenticity of an original data set and can be used as a digital \*547 equivalent of the Bates stamp used in paper document production.<sup>FN23</sup>”

FN23. Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, Federal Judicial Center, 2007 at 24; *see also Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 655 (D.Kan.2005).

Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4). Also, they can be used during discovery of electronic records to create a form of electronic “Bates stamp” that will help establish the document as electronic.<sup>FN24</sup> This underscores a point that counsel often overlook. A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the “final” or legally operative version. This can plague a party seeking to introduce a

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. Use of hash values when creating the “final” or “legally operative” version of an electronic record can insert distinctive characteristics into it that allow its authentication under Rule 901(b)(4).

FN24. See, e.g., United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 20, <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf> (last visited April 10, 2007) (encouraging parties to discuss use of hash values or “hash marks” when producing electronic records in discovery to facilitate their authentication).

Another way in which electronic evidence may be authenticated under Rule 901(b)(4) is by examining the metadata for the evidence. Metadata,

“commonly described as ‘data about data,’ is defined as ‘information describing the history, tracking, or management of an electronic document.’ Appendix F to *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* defines metadata as ‘information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).’ Technical Appendix E to the *Sedona Guidelines* provides an extended description of metadata. It further defines metadata to include ‘all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records.’ Some examples of metadata for electronic documents include: a file’s name, a file’s location (e.g., directory structure or pathname), file format or file type, file size, file

dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept.”

*Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. at 646 (footnote omitted); Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, Federal Judicial Center, 2007 at 24-25 (defining metadata as “[i]nformation about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified ...”). Recently revised Federal Rule of Civil Procedure 34 permits a party to discover electronically stored information and to identify the form or forms in which it is to be produced. A party therefore can request production of electronically stored information in its “native format”, which includes the metadata for the electronic document.<sup>FN25</sup> Because metadata shows the date, \*548 time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4). Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because,

FN25. United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 17, <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf> (last visited April 10, 2007) (“When parties have agreed or the Court has ordered the parties to exchange all or some documents as electronic files in Native File format in connection with discovery, the parties should

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

collect and produce said relevant files in Native File formats in a manner that preserves the integrity of the files, including, but not limited to the contents of the file, the Meta-Data (including System Meta-Data, Substantive Meta-Data, and Embedded Meta-Data....”).

“[a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide for a selected network administrators to override an individual password identification number to gain access when necessary.”

WEINSTEIN at § 900.01[4][a]; *see also Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 530 (1 st Cir.1996) (discussing how metadata markers can reflect that a document was modified when in fact it simply was saved to a different location). Despite its lack of conclusiveness, however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics.

**Rule 901(b)(7):**

This Rule permits authentication by:

“Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.”

The commentary to Rule 901(b)(7) recognizes that it applies to computerized public records, noting that “[p]ublic records are regularly authenticated by proof of custody, without more. [Rule 901(b)(7)] extends the principle to include data stored in computers and similar methods, of which increasing use in

the public records area may be expected.” FED.R.EVID. 901(b)(7) advisory committee's note (citation omitted). To use this rule the “proponent of the evidence need only show that the office from which the records were taken is the legal custodian of the records.” WEINSTEIN at § 901.10[2]. This may be done by “[a] certificate of authenticity from the public office; [t]he testimony of an officer who is authorized to attest to custodianship, [or] the testimony of a witness with knowledge that the evidence is in fact from a public office authorized to keep such a record.” *Id.* (footnote omitted). Examples of the types of public records that may be authenticated by Rule 901(b)(7) include tax returns, weather bureau records, military records, social security records, INS records, VA records, official records from federal, state and local agencies, judicial records, correctional records, law enforcement records, and data compilations, which may include computer stored records. *Id.*

Courts have recognized the appropriateness of authenticating computer stored public records under Rule 901(b)(7) as well, and observed that under this rule, unlike Rule 901(b)(9), there is no need to show that the computer system producing the public records was reliable or the records accurate. For example, in *United States v. Meienberg*, the court rejected defendant's challenge to the admissibility of a law enforcement agency's computerized records. Defendant argued that the only way they could be authenticated was under Rule 901(b)(9), through proof that they were produced by a system or process capable of producing a reliable result. Defendant further argued that the records had not been shown to be accurate. The appellate court disagreed, holding that the records properly had been authenticated under Rule 901(b)(7), which did not require a showing of accuracy. The court noted that any question regarding the accuracy of the records went to weight rather than admissibility. 263 F.3d at 1181. Thus, a decision to authenticate under Rule 901(b)(7), as opposed to 901(b)(9) may mean that the required foundation is much easier to prove. \*549 This underscores the importance of the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

point previously made, that there may be multiple ways to authenticate a particular computerized record, and careful attention to all the possibilities may reveal a method that significantly eases the burden of authentication.

**Rule 901(b)(9):**

This Rule recognizes one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. It authorizes authentication by “[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.” FED.R.EVID. 901(b)(9). This rule was “designed for situations in which the accuracy of a result is dependent upon a process or system which produces it.” FED.R.EVID. 901(b)(9) advisory committee’s note. *See also* WEINSTEIN at § 901.12[3]; <sup>FN26</sup> *In re Vee Vinhnee*, 336 B.R. at 446 (“Rule 901(b)(9), which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. The advisory committee note makes plain that Rule 901(b)(9) was designed to encompass computer-generated evidence ...”). <sup>FN27</sup>

FN26. “Computer output may be authenticated under Rule 901(b)(9).... When the proponent relies on the provisions of Rule 901(b)(9) instead of qualifying the computer-generated information for a hearsay exception, it is common for the proponent to provide evidence of the input procedures and their accuracy, and evidence that the computer was regularly tested for programming errors. At a minimum, the proponent should present evidence sufficient to warrant a finding that the information is trustworthy and provide the opponent with an opportunity to inquire into the accuracy of the computer and of the input procedures.”

FN27. In *Vinhnee*, the court cited with approval an eleven-step foundational authentication for computer records advocated by one respected academic. *Id.* (citing EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS 58-59 (LexisNexis 6th ed.2005)). Although this foundation is elaborate, and many courts might not be so demanding as to require that it be followed to authenticate computer generated records, the fact that one court already has done so should put prudent counsel on notice that they must pay attention to how they will authenticate computer generated records, and that they should be prepared to do so in a manner that complies with the Federal Rules of Evidence and any governing precedent. The price for failing to do so may be, as in *In re Vee Vinhnee*, exclusion of the exhibit. *See, e.g., Indianapolis Minority Contractors Ass’n, Inc. v. Wiley*, 1998 WL 1988826, at \*7 (S.D.Ind. May 13, 1998) (“[A]s a condition precedent to admissibility of computer records, the proponent must establish that the process or system used produces an accurate result, FED.R.EVID. 901(b)(9), and that foundation has not been established. In light of the above, the veracity and reliability of these reports are questionable, and thus [the summary judgment exhibit] will be stricken”).

**Rule 902:**

In addition to the non-exclusive methods of authentication identified in Rule 901(b), Rule 902 identifies twelve methods by which documents, including electronic ones, may be authenticated without extrinsic evidence. This is commonly referred to as “self-authentication.” The rule states:

“Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

(1) Domestic public documents under seal. A document bearing a seal purporting to be that of the United States, or of any State, district, Commonwealth, territory, or insular possession thereof, or the Panama Canal Zone, or the Trust Territory of the Pacific Islands, or of a political subdivision, department, officer, or agency thereof, and a signature purporting to be an attestation or execution.

(2) Domestic public documents not under seal. A document purporting to bear the signature in the official capacity of an officer or employee of any entity included in paragraph (1) hereof, having no seal, if a public officer having a seal and having official duties in the district or political subdivision of the officer or employee certifies under seal that the signer has the official capacity and that the signature is genuine.

(3) Foreign public documents. A document purporting to be executed or attested in an official capacity by a person authorized by the laws of a foreign country to make the execution or attestation, and accompanied by a final certification as to the \*550 genuineness of the signature and official position (A) of the executing or attesting person, or (B) of any foreign official whose certificate of genuineness of signature and official position relates to the execution or attestation or is in a chain of certificates of genuineness of signature and official position relating to the execution or attestation. A final certification may be made by a secretary of an embassy or legation, consul general, consul, vice consul, or consular agent of the United States, or a diplomatic or consular official of the foreign country assigned or accredited to the United States. If reasonable opportunity has been given to all parties to investigate the authenticity and accuracy of official documents, the court may, for good cause shown, order that they be treated as presumptively authentic without final certification or permit them to be evidenced by an attested summary with or

without final certification.

(4) Certified copies of public records. A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.

(6) Newspapers and periodicals. Printed materials purporting to be newspapers or periodicals.

(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.

(8) Acknowledged documents. Documents accompanied by a certificate of acknowledgment executed in the manner provided by law by a notary public or other officer authorized by law to take acknowledgments.

(9) Commercial paper and related documents. Commercial paper, signatures thereon, and documents relating thereto to the extent provided by general commercial law.

(10) Presumptions under Acts of Congress. Any signature, document, or other matter declared by Act of Congress to be presumptively or prima facie genuine or authentic.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

(11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

(12) Certified foreign records of regularly conducted activity. In a civil case, the original or a duplicate of a foreign record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration by its custodian or other qualified person certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

\*551 (B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

The declaration must be signed in a manner that, if falsely made, would subject the maker to criminal penalty under the laws of the country where the declaration is signed. A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them."

The obvious advantage of Rule 902 is that it does not require the sponsoring testimony of any witness to authenticate the exhibit—its admissibility is determined simply by examining the evidence itself, along with any accompanying written declaration or certificate required by Rule 902. The mere fact that the rule permits self-authentication, however, does not foreclose the opposing party from challenging the authenticity. Because Rule 104(b) applies in such cases, the exhibit and the evidence challenging its authenticity goes to the jury, which ultimately determines whether it is authentic. FED.R.EVID. 902 advisory committee's note. Some of the examples contained in Rule 902, such as Rule 902(3) (foreign public documents), 902(4) (certified copies of public records), 902(8) (acknowledged documents), 902(11) (certified copies of domestic records of a regularly conducted activity), and 902(12) (certified foreign records of regularly conducted activity), do require a certificate signed by a custodian or other qualified person to accomplish the self-authentication.

Although all of the examples contained in Rule 902 could be applicable to computerized records, three in particular have been recognized by the courts to

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

authenticate electronic evidence: 902(5) (official publications); 902(7) (trade inscriptions); and, 902(11) (certified domestic records of regularly conducted activity). The first, Rule 902(5), provides:

“(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.”

The rule “[dispenses] with preliminary proof of the genuineness of purportedly official publications .... [but] does not confer admissibility upon all official publications; it merely provides a means whereby their authenticity may be taken as established for purposes of admissibility.” FED.R.EVID. 902(5) advisory committee's note. This means that, to be admissible, the proponent may also need to establish that the official record qualifies as a public record hearsay exception under Rule 803(8). WEINSTEIN at § 902.02[2]. Although the rule is silent regarding the level of government that must authorize the publication, commentators suggest that the list includes the United States, any State, district, commonwealth, territory or insular possession of the United States, the Panama Canal Zone, the Trust Territory of the Pacific islands, or a political subdivision, department, officer, or agency of any of the foregoing. *Id.*

In *Equal Employment Opportunity Commission v. E.I. DuPont de Nemours and Co.*, the court admitted into evidence printouts of postings on the website of the United States Census Bureau as self-authenticating under Rule 902(5). 2004 WL 2347556 (E.D.La. Oct.18, 2004). Given the frequency with which official publications from government agencies are relevant to litigation and the increasing tendency for such agencies to have their own websites, Rule 902(5) provides a very useful method of authenticating these publications. When combined with the public records exception to the hearsay rule, Rule 803(8), these official publications posted on government agency websites should be admitted into evidence easily.

Rule 902(7) provides that exhibits may be self-authenticated by “[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.” As one commentator has noted, “[u]nder Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the \*552 employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7).” WEINSTEIN at § 900.07[3][c].

Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness to testify in person at trial. It provides:

“(11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.”

This rule was added in the 2000 amendments to the Federal Rules of Evidence, and it was intended to “[set] forth a procedure by which parties can authenticate certain records of regularly conducted activity, other than through the testimony of a foundation witness.” FED.R.EVID. 902(11) advisory committee’s note. Unlike most of the other authentication rules, Rule 902(11) also contains a notice provision, requiring the proponent to provide written notice of the intention to use the rule to all adverse parties and to make available to them the records sufficiently in advance of litigation to permit a fair opportunity to challenge them. WEINSTEIN at § 902.13[2]. Because compliance with Rule 902(11) requires the proponent to establish all the elements of the business record exception to the hearsay rule, Rule 803(6), courts usually analyze the authenticity issue under Rule 902(11) concomitantly with the business record hearsay exception.<sup>FN28</sup> *Rambus*, 348 F.Supp.2d at 701 (“Thus, the most appropriate way to view Rule 902(11) is as the functional equivalent of testimony offered to authenticate a business record tendered under Rule 803(6) because the declaration permitted by Rule 902(11) serves the same purpose as authenticating testimony ... [B]ecause Rule 902[11] contains the same requirements, and almost the same wording, as Rule 803(6), decisions explaining the parallel provisions of Rule 803(6) are helpful in resolving the issues here presented.”); *In re Vee Vinhnee*, 336 B.R. at 444 (stating that in deciding whether to admit business records, the authenticity analysis is merged into the business record analysis).

FN28. Because the business record exception will be discussed at some length below, the analysis of the requirements of Rule 902(11)

will be deferred until that discussion.

Finally, as noted at the beginning of this discussion regarding the authenticating electronic records, Rule 901(b) makes clear that the ten examples listed are illustrative only, not exhaustive. In ruling on whether electronic evidence has been properly authenticated, courts have been willing to think “outside of the box” to recognize new ways of authentication. For example, they have held that documents provided to a party during discovery by an opposing party are presumed to be authentic, shifting the burden to the producing party to demonstrate that the evidence that they produced was not authentic. *Indianapolis Minority Contractors Ass’n*, 1998 WL 1988826, at \*6 (“The act of production is an implicit authentication of documents produced.... Federal Rule of Evidence 901 provides that ‘[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. Defendants admit that they did produce [the exhibits at issue].... Thus ... the \*553 Defendants cannot have it both ways. They cannot voluntarily produce documents and implicitly represent their authenticity and then contend they cannot be used by the Plaintiffs because the authenticity is lacking.” (citation omitted)); *Perfect 10*, 213 F.Supp.2d at 1153-54 (finding that exhibits of website postings had been properly authenticated for three reasons, including that certain of them had been provided to the plaintiff by the defendant during discovery).

In *Telewizja Polska USA*, the court embraced a non-traditional method of authentication when faced with determining whether exhibits depicting the content of the defendant’s website at various dates several years in the past were admissible. 2004 WL 2367740. The plaintiff offered an affidavit from a representative of the Internet Archive Company, which retrieved copies of the defendant’s website as it appeared at relevant dates to the litigation through use of its “wayback machine.”<sup>FN29</sup> The defendant objected,

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

contending that the Internet Archive was not a reliable source, and thus the exhibits had not been authenticated. The court disagreed, stating:

FN29. The “wayback machine” refers to the process used by the Internet Archive Company, [www.archive.org](http://www.archive.org), to allow website visitors to search for archived web pages of organizations. *St. Luke's*, 2006 WL 1320242 at \*1.

“Federal Rule of Evidence 901 ‘requires only a prima facie showing of genuineness and leaves it to the jury to decide the true authenticity and probative value of the evidence.’ Admittedly, the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in Rule 901; the Internet Archive is a relatively new source for archiving websites. Nevertheless, Plaintiff has presented no evidence that the Internet Archive is unreliable or biased. And Plaintiff has neither denied that the exhibit represents the contents of its website on the dates in question, nor come forward with its own evidence challenging the veracity of the exhibit. Under these circumstances, the Court is of the opinion that [the affidavit from the representative of the Internet Archive Company] is sufficient to satisfy Rule 901’s threshold requirement for admissibility.”

*Id.* at \*6.

Additionally, authentication may be accomplished by the court taking judicial notice under Rule 201 of certain foundational facts needed to authenticate an electronic record. Under this rule, the parties may request the court to take judicial notice of adjudicative facts that are either (1) generally known within the territorial jurisdiction of the trial court, or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. FED.R.EVID. 201(b); WEINSTEIN at § 201.12[1]. Judicial notice could be a helpful way to establish certain well known characteristics of com-

puters, how the internet works, scientific principles underlying calculations performed within computer programs, and many similar facts that could facilitate authenticating electronic evidence.

Authentication also can be accomplished in civil cases by taking advantage of FED.R.CIV.P. 36, which permits a party to request that his or her opponent admit the “genuineness of documents.” Also, at a pretrial conference, pursuant to FED.R.CIV.P. 16(c)(3), a party may request that an opposing party agree to stipulate “regarding the authenticity of documents,” and the court may take “appropriate action” regarding that request. Similarly, if a party properly makes his or her FED. R. CIV. P. 26(a)(3) pretrial disclosures of documents and exhibits, then the other side has fourteen days in which to file objections. Failure to do so waives all objections other than under Rules 402 or 403, unless the court excuses the waiver for good cause. This means that if the opposing party does not raise authenticity objections within the fourteen days, they are waived.

The above discussion underscores the need for counsel to be creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in Rules 901 and 902 that neatly fits.

Finally, any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the \*554 wide diversity of such evidence, there is no single approach to authentication that will work in all instances. It is possible, however, to identify certain authentication issues that have been noted by courts and commentators with particular types of electronic evidence and to be forearmed with this knowledge to develop authenticating facts that address these concerns.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

#### E-mail

There is no form of ESI more ubiquitous than e-mail, and it is the category of ESI at issue in this case. Although courts today have more or less resigned themselves to the fact that “[w]e live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world,” *Safavian*, 435 F.Supp.2d at 41, it was not very long ago that they took a contrary view—“[e]-mail is far less of a systematic business activity than a monthly inventory printout.” *Monotype Corp. PLC v. Int'l Typeface*, 43 F.3d 443, 450 (9th Cir.1994) (affirming trial court's exclusion of e-mail as inadmissible as a business record). Perhaps because of the spontaneity and informality of e-mail, people tend to reveal more of themselves, for better or worse, than in other more deliberative forms of written communication. For that reason, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved. Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence. *See, e.g., Safavian*, 435 F.Supp.2d 36.

Not surprisingly, there are many ways in which e-mail evidence may be authenticated. One well respected commentator has observed:

“[E]-mail messages may be authenticated by direct or circumstantial evidence. An e-mail message's distinctive characteristics, including its ‘contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances’ may be sufficient for authentication.

Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the

message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender's listed e-mail address.

The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message.

E-mails may even be self-authenticating. Under Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7). However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.”

WEINSTEIN at § 900.07[3][c]; *see also* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[4][b] (LexisNexis 6th ed.2005)(hereinafter “IMWINKELRIED, EVIDENTIARY FOUNDATIONS.”) Courts also have approved the authentication of e-mail by the above described methods. *See, e.g., Siddiqui*, 235 F.3d at 1322-23 (E-mail may be authenticated entirely by circumstantial evidence, including its distinctive characteristics); *Safavian*, 435 F.Supp.2d at 40 (recognizing that e-mail may be authenticated by distinctive characteristics 901(b)(4), or by comparison of exemplars with other e-mails that already have been authenticated 901(b)(3)); *Rambus*, 348 F.Supp.2d 698 (E-mail that qualifies as business record may be \*555 self-authenticating under 902(11)); *In re F.P.*, 878

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

A.2d at 94 (E-mail may be authenticated by direct or circumstantial evidence).

The most frequent ways to authenticate e-mail evidence are 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), 901(b)(4) (distinctive characteristics, including circumstantial evidence), 902(7) (trade inscriptions), and 902(11) (certified copies of business record).

### Internet Website Postings

Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation. Their reaction has ranged from the famous skepticism expressed in *St. Clair v. Johnny's Oyster and Shrimp, Inc.* 76 F.Supp.2d 773 (S.D.Tex.1999),<sup>FN30</sup> to more permissive approach taken in *Perfect 10*, 213 F.Supp.2d at 1153-54.<sup>FN31</sup>

FN30. There, the court stated that,

"Plaintiff's electronic 'evidence' is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and

*nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in FED.R.EVID. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form from the United States Coast Guard or discover alternative information verifying what Plaintiff alleges."

*Id.* at 774-775.

FN31. The court noted that 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.

The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting. See *United States v. Jackson*, 208 F.3d 633, 638 (7th

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

Cir.2000) (excluding evidence of website postings because proponent failed to show that sponsoring organization actually posted the statements, as opposed to a third party); *St. Luke's*, 2006 WL 1320242 (plaintiff failed to authenticate exhibits of defendant's website postings because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website); *Wady*, 216 F.Supp.2d 1060. One commentator has observed “[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?”<sup>FN32</sup> The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

FN32. Joseph at 21; *see also* SALTZBURG at § 901.02[12].

“The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data \*556 has been republished by others who identify the source of the data as the website in question?”<sup>FN33</sup>

FN33. *Id.* at 22.

Counsel attempting to authenticate exhibits containing information from internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation. The authentication rules most likely to

apply, singly or in combination, are 901(b)(1) (witness with personal knowledge) 901(b)(3) (expert testimony) 901(b)(4) (distinctive characteristics), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications).

### Text Messages and Chat Room Content

Many of the same foundational issues found encountered when authenticating website evidence apply with equal force to text messages and internet chat room content; however, the fact that chat room messages are posted by third parties, often using “screen names” means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host. SALTZBURG at § 901.02[12]. One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

“(1) [e]vidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);

(2) [e]vidence that, when a meeting with the person using the screen name was arranged, the individual ... showed up; (3) [e]vidence that the person using the screen name identified [himself] as the [person in the chat room conversation]; evidence that the individual had in [his] possession information given to the person using the screen name; (5) [and][e]vidence from the hard drive of the individual's computer [showing use of the same screen name].”

*Id.* at § 901.02[12]. Courts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. For example, in *In re F.P.*, the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. 878 A.2d at 93-94. The court held that

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts. *Id.* Similarly, in *United States v. Simpson*, the court held that there was ample circumstantial evidence to authenticate printouts of the content of chat room discussions between the defendant and an undercover detective, including use of the e-mail name of the defendant, the presence of the defendant's correct address in the messages, and notes seized at the defendant's home containing the address, e-mail address and telephone number given by the undercover officer. 152 F.3d at 1249. Likewise, in *United States v. Tank*, the court found sufficient circumstantial facts to authenticate chat room conversations, despite the fact that certain portions of the text of the messages in which the defendant had participated had been deleted. 200 F.3d at 629-31. There, the court found the testimony regarding the limited nature of the deletions by the member of the chat room club who had made the deletions, circumstantial evidence connecting the defendant to the chat room, including the use of the defendant's screen name in the messages, were sufficient to authenticate the messages. *Id.* at 631. Based on the foregoing cases, the rules most likely to be used to authenticate chat room and text messages, alone or in combination, appear to be 901(b)(1) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics).

#### Computer Stored Records and Data

Given the widespread use of computers, there is an almost limitless variety of records that are stored in or generated by computers. As one commentator has observed "[m]any kinds of computer records and computer-generated information are introduced as real evidence or used as litigation aids at trials. They range from computer printouts \*557 of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements." WEINSTEIN at §

900.06[3]. The least complex admissibility issues are associated with electronically stored records. "In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues." WEINSTEIN at § 900.06[3]. That said, although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional "hard copy" records. MANUAL FOR COMPLEX LITIGATION at § 11.447; <sup>FN34</sup> see also IMWINKELRIED, EVIDENTIARY FOUNDATIONS at 4.03[2].<sup>FN35</sup>

FN34. "Computerized data", however, 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.

"The judge should therefore consider the accuracy and reliability of computerized evidence...."

FN35. "In the past, many courts have been lax in applying the authentication requirement to computer records; they have been content with foundational evidence that the business has successfully used the computer system in question and that the witness recognizes the record as output from the computer. However, following the recommendations of the Federal Judicial Center's *Manual for Complex Litigation*, some courts now require more extensive foundation. These courts require the proponent to authenticate a

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

computer record by proving the reliability of the particular computer used, the dependability of the business's input procedures for the computer, the use of proper procedures to obtain the document offered in court, and the witness's recognition of that document as the readout from the computer." (citation omitted).

Two cases illustrate the contrast between the more lenient approach to admissibility of computer records and the more demanding one. In *United States v. Meienberg*, the defendant challenged on appeal the admission into evidence of printouts of computerized records of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records. 263 F.3d at 1180-81. The Tenth Circuit disagreed, stating:

"Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility."

*Id.* at 1181 (citation omitted). *See also Kassimu*, 2006 WL 1880335 (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 Rule 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); *Sea-Land Serv., Inc. v. Lozen Int'l*, 285 F.3d 808 (9th Cir.2002) (ruling that trial court properly considered electronically generated bill of lading as an exhibit to a summary judgment motion. The only foundation that was required was that the record was produced from the same electronic information that was generated contemporaneously when the parties entered into their contact.

The court did not require evidence that the records were reliable or accurate).

In contrast, in the case of *In re Vee Vinhnee*, the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. 336 B.R. 437. The court noted that "it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground." *Id.* at 445-46. The court further observed that:

"The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the \*558 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.... Hence, 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."

*Id.* at 444. The court reasoned that, for paperless electronic records:

"The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation."

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

*Id.* at 445. In order to meet the heightened demands for authenticating electronic business records, the court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried:<sup>FN36</sup>

FN36. IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.03[2].

Professor Imwinkelried perceives electronic records as a form of scientific evidence and discerns an eleven-step foundation for computer records:

- “1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.

11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.”

*Id.* at 446-47 (citation omitted). Although the position taken by the court in *In re Vee Vinhnee* appears to be the most demanding requirement for authenticating computer stored records, other courts also have recognized a need to demonstrate the accuracy of these records. *See, e.g., State v. Dunn*, 7 S.W.3d 427, 432 (Mo.Ct.App.2000) (Admissibility of computer-generated records “should be determined on the basis of the reliability and accuracy of the process involved.”); *State v. Hall*, 976 S.W.2d 121, 147 (Tenn.1998) ( “[T]he admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.”).<sup>FN37</sup>

FN37. In addition to their insight regarding the authentication of electronic records, these cases are also important in connection to the analysis of whether certain types of electronically stored records constitute hearsay when offered for their substantive truth.

As the foregoing cases illustrate, there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed. Further, it would not be surprising to find that, to date, more courts have tended towards the lenient rather than the demanding approach. However, it also is plain that commentators and courts increasingly recognize the special characteristics of electronically stored records, and there appears to be a growing awareness, as expressed in the *Manual for Complex Litigation*,<sup>FN38</sup> that courts “should ... consider the accuracy and reliability of computerized evidence” in ruling on \*559 its admissibility. Lawyers can expect to encounter judges in both camps, and in

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Further, although “it may be better to be lucky than good,” as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.

#### FN38. MANUAL FOR COMPLEX LITIGATION at § 11.446.

The methods of authentication most likely to be appropriate for computerized records are 901(b)(1) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), and 901(b)(9) (system or process capable of producing a reliable result).

#### Computer Animation and Computer Simulations.

Two similar, although distinct, forms of computer generated evidence also raise unique authentication issues. The first is computer animation, “the display of a sequence of computer-generated images.” IM-WINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a]. The attraction of this form of evidence is irresistible, because:

“when there is no movie or video of the event being litigated, a computer animation is a superior method of communicating the relevant information to the trier of fact. Absent a movie or video, the proponent might have to rely on static charts or oral testimony to convey a large amount of complex information to the trier of fact. When the proponent relies solely on oral expert testimony, the details may be presented one at a time; but an animation can piece all the details together for the jury. A computer animation in effect condenses the information into a single

evidentiary package. In part due to television, the typical American is a primarily visual learner; and for that reason, in the short term, many jurors find the animation more understandable than charts or oral testimony. Use of an animation can also significantly increase long-term juror retention of the information.”

*Id.* at § 4.09[4][a]. The second form of computer generated evidence is a computer simulation. The distinction between them has been explained usefully as follows:

“Computer generated evidence is an increasingly common form of demonstrative evidence. If the purpose of the computer evidence is to illustrate and explain a witness's testimony, courts usually refer to the evidence as an animation. In contrast, a simulation 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, and courts generally require proof to show the validity of the science before the simulation evidence is admitted.”

Thus, the classification of a computer-generated exhibit as a simulation or an animation also affects the evidentiary foundation required for its admission.

*State v. Sayles*, 662 N.W.2d 1, 9 (Iowa 2003) (citation omitted).

Courts generally have allowed the admission of computer animations if authenticated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help to illustrate the testimony given in the case. This usually is the sponsoring witness. *Id.* at 10 (state's expert witness had knowledge of content of shaken infant syndrome animation and could testify that it correctly and adequately portrayed the facts that would illustrate her

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

testimony); *Hinkle v. City of Clarksburg*, 81 F.3d 416 (4th Cir.1996) (holding that a computer-animated videotaped recreation of events at issue in trial is not unduly prejudicial if it is sufficiently close to the actual events and is not confused by the jury for the real life events themselves); *Friend v. Time Mfg. Co.*, 2006 WL 2135807, at \*7 (D.Ariz. July 28, 2006) (“The use of computer animations is allowed when it satisfies the usual foundational requirements for demonstrative evidence. ‘At a minimum, the animation’s proponent must show the computer simulation fairly and accurately depicts \*560 what it represents, whether through the computer expert who prepared it or some other witness who is qualified to so testify, and the opposing party must be afforded an opportunity for cross-examination.’ ” (citation omitted)); *People v. Cauley*, 32 P.3d 602 (Colo.App.2001) (holding that, “[a] computer animation is admissible as demonstrative evidence if the proponent of the video proves that it: 1) is authentic ...; 2) is relevant ...; 3) is a fair and accurate representation of the evidence to which it relates; and 4) has a probative value that is not substantially outweighed by the danger of unfair prejudice ...”); *Clark v. Cantrell*, 339 S.C. 369, 529 S.E.2d 528 (2000) (“[A] party may authenticate a video animation by offering testimony from a witness familiar with the preparation of the animation and the data on which it is based ... [including] the testimony of the expert who prepared the underlying data and the computer technician who used that data to create it.” (citation omitted)). Thus, the most frequent methods of authenticating computer animations are 901(b)(1) (witness with personal knowledge), and 901(b)(3) (testimony of an expert witness).

Computer simulations are treated as a form of scientific evidence, offered for a substantive, rather than demonstrative purpose. WEINSTEIN at § 900.03[1] (p. 900-21); IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a], [c]. The case most often cited with regard to the foundational requirements needed to authenticate a computer simulation is *Commercial Union v. Boston Edison*, where

the court stated:

“The function of computer programs like TRACE ‘is to perform rapidly and accurately an extensive series of computations not readily accomplished without use of a computer.’ We permit experts to base their testimony on calculations performed by hand. There is no reason to prevent them from performing the same calculations, with far greater rapidity and accuracy, on a computer. Therefore ... we treat computer-generated models or simulations like other scientific tests, and condition admissibility on a sufficient showing that: (1) the computer is functioning properly; (2) the input and underlying equations are sufficiently complete and accurate (and disclosed to the opposing party, so that they may challenge them); and (3) the program is generally accepted by the appropriate community of scientists.”

412 Mass. 545, 591 N.E.2d 165, 168 (1992) (citation omitted). The *Commercial Union* test has been followed by numerous courts in determining the foundation needed to authenticate computer simulations. For example, in *State v. Swinton*, the court cited with approval *Commercial Union*, but added that the key to authenticating computer simulations is to determine their reliability. 268 Conn. 781, 847 A.2d 921, 942 (2004). In that regard, the court noted that the following problems could arise with this type of computer evidence: (1) the underlying information itself could be unreliable; (2) the entry of the information into the computer could be erroneous; (3) the computer hardware could be unreliable; (4) the computer software programs could be unreliable; (5) “the execution of the instructions, which transforms the information in some way—for example, by calculating numbers, sorting names, or storing information and retrieving it later” could be unreliable; (6) the output of the computer—the printout, transcript, or graphics, could be flawed; (7) the security system used to control access to the computer could be compromised; and (8) the user of the system could make errors. The

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

court noted that Rule 901(b)(9) was a helpful starting point to address authentication of computer simulations. *Id.*; see also *Bray v. Bi-State Dev. Corp.*, 949 S.W.2d 93 (Mo.Ct.App.1997) (citing *Commercial Union* and ruling that authentication properly was accomplished by a witness with knowledge of how the computer program worked, its software, the data used in the calculations, and who verified the accuracy of the calculations made by the computer with manual calculations); *Kudlacek v. Fiat*, 244 Neb. 822, 509 N.W.2d 603, (1994) (citing *Commercial Union* and holding that computer simulation was authenticated by the plaintiff's expert witness). Thus, the most frequent methods of authenticating computer simulations are 901(b)(1) (witness with personal knowledge); and 901(b)(3) (expert witness). Use of an expert witness to authenticate a computer simulation likely will also \*561 involve Federal Rules of Evidence 702 and 703.

### Digital Photographs

Photographs have been authenticated for decades under Rule 901(b)(1) by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately represents the scene. Calling the photographer or offering expert testimony about how a camera works almost never has been required for traditional film photographs. Today, however, the vast majority of photographs taken, and offered as exhibits at trial, are digital photographs, which are not made from film, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered. Indeed, unlike photographs made from film, digital photographs may be "enhanced." Digital image "enhancement consists of removing, inserting, or highlighting an aspect of the photograph that the technician wants to change." Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005, at 48. Some examples graphically illustrate the authentication issues associated with digital enhancement of photographs:

"[S]uppose that in a civil case, a shadow on a 35 mm photograph obscures the name of the manufacturer of an offending product. The plaintiff might offer an enhanced image, magically stripping the shadow to reveal the defendant's name. Or suppose that a critical issue is the visibility of a highway hazard. A civil defendant might offer an enhanced image of the stretch of highway to persuade the jury that the plaintiff should have perceived the danger ahead before reaching it. In many criminal trials, the prosecutor offers an 'improved', digitally enhanced image of fingerprints discovered at the crime scene. The digital image reveals incriminating points of similarity that the jury otherwise would never would have seen."

*Id.* at 49. There are three distinct types of digital photographs that should be considered with respect to authentication analysis: original digital images, digitally converted images, and digitally enhanced images. *Id.*

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. *Id.* If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under Rule 201. *Id.* 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, Rules 901(b)(1) and 901(b)(9)-the later rule implicating expert testimony under Rule 702. *Id.* Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion. *Id.*

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

For digitally enhanced images, 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 Rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under Rule 702. *Id.* Recently, one state court has given particular scrutiny to how this should be done. In *State v. Swinton*, the defendant was convicted of murder in part based on evidence of computer enhanced images prepared using the Adobe Photoshop software. 268 Conn. 781, 847 A.2d 921, 950-52 (2004). The images showed a superimposition of the defendants teeth over digital photographs of bite marks taken from the victim's body. At trial, the state called the forensic odontologist (bite mark expert) to testify that the defendant was the source of the bite marks on the victim. However, the defendant testified that he was not familiar with how the Adobe Photoshop made the overlay photographs, which involved\*562 a multi-step process in which a wax mold of the defendant's teeth was digitally photographed and scanned into the computer to then be superimposed on the photo of the victim. The trial court admitted the exhibits over objection, but the state appellate court reversed, finding that the defendant had not been afforded a chance to challenge the scientific or technical process by which the exhibits had been prepared. The court stated that to authenticate the exhibits would require a sponsoring witness who could testify, adequately and truthfully, as to exactly what the jury was looking at, and the defendant had a right to cross-examine the witness concerning the evidence. Because the witness called by the state to authenticate the exhibits lacked the computer expertise to do so, the defendant was deprived of the right to cross examine him. *Id.* at 950-51.

Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a

means to authenticate digitally enhanced photographs under Rule 901(b)(9): (1) The witness is an expert in digital photography; (2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the process by which the computer manipulates them; (3) the witness testifies that the processes used are valid; (4) the witness testifies that there has been "adequate research into the specific application of image enhancement technology involved in the case"; (5) the witness testifies that the software used was developed from the research; (6) the witness received a film photograph; (7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer; (8) the witness can identify the trial exhibit as the product of the enhancement process he or she performed. Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005 at 54. The author recognized that this is an "extensive foundation," and whether it will be adopted by courts in the future remains to be seen. *Id.* However, it is probable that courts will require authentication of digitally enhanced photographs by adequate testimony that it is the product of a system or process that produces accurate and reliable results. FED.R.EVID. 901(b)(9).

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced. Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in Rules 901 and 902, as well as consider requesting a stipulation from opposing counsel, or filing a request for admission of the genuineness of the evidence under Rule 36 of the Federal Rules of Civil Procedure. With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be spe-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

cific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

In this case, neither plaintiffs nor defendants provided any authenticating facts for the e-mail and other evidence that they proffered in support of their summary judgment memoranda—they simply attached the exhibits. This complete absence of authentication stripped the exhibits of any evidentiary value because the Court could not consider them as evidentiary facts. This, in turn, required the dismissal, without prejudice, of the cross motions for summary judgment, with leave to resubmit them once the evidentiary deficiencies had been cured.

#### *Hearsay (Rules 801-807)*

The fourth “hurdle” that must be overcome when introducing electronic evidence is the potential application of the hearsay rule. Hearsay issues are pervasive when electronically stored and generated evidence is introduced. To properly analyze hearsay issues there are five separate questions that must be answered: (1) does the evidence constitute a **statement**, as defined by Rule 801(a); (2) was the statement made by a “**declarant**,” as defined by Rule 801(b); (3) is the statement being offered to prove the **truth of its contents**, as provided by Rule 801(c); \*563 (4) is the statement **excluded from the definition of hearsay by rule 801(d)**; and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807. It is critical to proper hearsay analysis to consider each of these questions.

#### *The requirements of a “Statement,” Rule 801(a), made by a “Person”, Rule 801(b)*

Rule 801(a) states:

“A ‘statement’ is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion.”

The key to understanding the hearsay rule is to appreciate that it only applies to intentionally assertive verbal or non-verbal conduct, and its goal is to guard against the risks associated with testimonial evidence: perception, memory, sincerity and narration. FED.R.EVID. 801 advisory committee's note (“The factors to be considered in evaluating the testimony of a witness are perception, memory, and narration. Sometimes a fourth is added, sincerity.”) (citations omitted); WEINSTEIN at § 801. 11[1] (“To be considered hearsay, a statement out of court must be offered in evidence to prove the truth of the matter it asserts. This part of the definition arises out of the factfinder's need to assess the credibility of the person who made a statement offered for its truth. When a witness testifies in court, the trier can assess the witness's perception, narration and memory to determine whether the testimony accurately represents the facts observed.”); PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE, 262 (ABA Publishing 2005)(hereinafter “RICE”) (“Hearsay is an out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination.”).

The use of the word “statement” in Rule 801(a) is a critical component of the hearsay rule. WEINSTEIN at § 801.10[1] (“Because Rule 801 describes hearsay as an out-of-court *statement* offered as proof as [sic] the matter asserted, the definition of ‘statement’ is of critical importance.”); SALTZBURG at § 801.02[1][c] (“If proffered evidence is not a ‘statement’ within the meaning of Rule 801(a), then it cannot be hearsay, and so cannot be excluded under the [hearsay] Rule.”). The word is used in a very precise, and non-colloquial sense—it only applies to verbal

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

conduct (spoken or written) or non-verbal conduct that is intended by a human declarant to be *assertive*. The advisory committee note to Rule 801(a) states this concept squarely:

“The definition of ‘statement’ assumes importance because the term is used in the definition of hearsay in subdivision (c). The effect of the definition of ‘statement’ is to exclude from the operation of the hearsay rule all evidence of conduct, verbal or nonverbal, not intended as an assertion. The key to the definition is that nothing is an assertion unless intended to be one.”

Ironically, the word “assertion” is not defined in the hearsay rule, despite its importance to the concept. An assertion usefully may be defined as “to state as true; declare; maintain.” Black’s Law Dictionary 106 (5th ed.1979).

Although there is not universal agreement on this point, it appears that for verbal or nonverbal conduct to fall within the definition of the hearsay rule as defined under the federal rules of evidence, it must be either an expressly assertive written or spoken utterance, or nonverbal conduct expressly intended to be an assertion—the federal rules appear to have excluded from the definition of hearsay “implied assertions”—or unstated assertions that are inferred from verbal or nonverbal conduct. The advisory committee’s note to Rule 801(a) supports the notion non-verbal conduct that is not assertive, and verbal conduct (spoken or written)<sup>FN39</sup> that is non-assertive should be viewed the same \*564 way—falling outside the definition of a “statement.”

FN39. An example of nonassertive written verbal conduct would be to write a person’s name and address on an envelope. An example of nonassertive spoken verbal conduct would be to ask a question that does not contain within it a factual assertion “Is it

going to rain tomorrow?”

“[N]onverbal conduct ... may be offered as evidence that the person acted as he did because of his belief in the existence of the condition sought to be proved, from which belief the existence of the condition may be inferred. This sequence is, arguably, in effect an assertion of the existence of the condition and hence properly includable within the hearsay concept. Admittedly, evidence of this character is untested with respect to the perception, memory, and narration (or their equivalents) of the actor, but the Advisory Committee is of the view that these dangers are minimal in the absence of an intent to assert and do not justify the loss of the evidence on hearsay grounds. No class of evidence is free of the possibility of fabrication, but the likelihood is less with nonverbal than with assertive verbal conduct. The situations giving rise to the nonverbal conduct are such as virtually to eliminate questions of sincerity.... *Similar considerations govern nonassertive verbal conduct and verbal conduct which is assertive but offered as a basis for inferring something other than the matter asserted, also excluded from the definition of hearsay by the language of subdivision (c).*”

FED.R.EVID. 801(a) advisory committee’s note (emphasis added) (citation omitted); *Wilson v. Clancy*, 747 F.Supp. 1154, 1158 (D.Md.1990) (“It appears to be the intent of the limitation of the hearsay definition under FED.R.EVID. 801(a)(2) to non-verbal conduct ‘intended by the [declarant] as an assertion’ to do away with the notion that ‘implied assertions’ are within the hearsay prohibition.” (alterations in original) (citation omitted)); WEINSTEIN at § 801.10[2][c];<sup>FN40</sup> SALTZBURG at § 801.02[1][c].<sup>FN41</sup>

FN40. “Words and actions may convey meaning even though they were not consciously intended as assertions. Sometimes the relevance of words or actions to show a particular fact depends on drawing an infer-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

ence that a person would not have spoken or acted in a certain way unless the person believed a relevant fact to be true. According to the Advisory Committee, the 'key to the definition is that nothing is an assertion unless it is intended to be'. Many courts have found that words or conduct offered to show the actor's implicit beliefs do not constitute statements under the hearsay rule unless they were intended by the actor as an assertion.... Other courts, however, have noted that an oral or written declaration is hearsay if offered to show the truth of a matter implied by its contents."

FN41. "Common-law jurisdictions divide on whether nonverbal conduct that is not intended as an assertion is hearsay if it is introduced to show the truth of the actor's underlying beliefs.... The reasons for excluding non-assertive conduct from the hearsay rule are persuasive. A principal reason for excluding hearsay is that the veracity of the declarant cannot be tested by cross-examination. In the case of non-assertive acts, the actor by definition does not intend to make an assertion, meaning that the risk of insincerity is substantially diminished. The actor is at least not trying to lie. Moreover, non-assertive conduct is usually more reliable than the ordinary out-of-court statement, because by conduct the declarant has risked action on the correctness of his belief-he has put his money where his mouth is."

The second question that must be answered in the hearsay analysis is closely tied to the first. A writing or spoken utterance cannot be a "statement" under the hearsay rule unless it is made by a "declarant," as required by Rule 801(b), which provides "[a] 'declarant' is a *person* who makes a statement." (emphasis added). When an electronically generated rec-

ord is entirely the product of the functioning of a computerized system or process, such as the "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no "person" involved in the creation of the record, and no "assertion" being made. For that reason, the record is not a statement and cannot be hearsay.

Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements" under Rule 801(a). Where the writings are non-assertive, or not made by a "person," courts have held that they do not constitute hearsay, as they are not "statements." *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.2003) ("[N]either the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by "a person," so nothing "said" by a machine ... is hearsay' " (second alteration in original)); \*565 *Safavian*, 435 F.Supp.2d at 44 (holding that portions of e-mail communications that make imperative statements instructing defendant what to do, or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay); *Telewizja Polska USA*, 2004 WL 2367740 (finding that images and text posted on website offered to show what the website looked like on a particular day were not "statements" and therefore fell outside the reach of the hearsay rule); *Perfect 10*, 213 F.Supp.2d at 1155 (finding that images and text taken from website of defendant not hearsay, "to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all-and thus fall outside the ambit of the hearsay rule."); *United States v. Rollins, rev'd on other grounds* 2004 WL 26780, at \*9 (A.F.Ct.Crim.App. Dec.24, 2003) ("Computer 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

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

admissibility of the computer tracing system record should be measured by the reliability of the system itself, relative to its proper functioning and accuracy.”); *State v. Dunn*, 7 S.W.3d 427, 432 (Mo.Ct.App.2000) (“Because records of this type [computer generated telephone records] are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the reliability and accuracy of the process involved.”); *State v. Hall*, 976 S.W.2d 121, 147 (Tenn.1998) (reviewing the admissibility of computer generated records and holding “[t]he 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.”).

***The requirement that the statement be offered to prove its substantive truth.***

The third question that must be answered in determining if evidence is hearsay is whether the statement is offered to prove its substantive truth, or for some other purpose. Rule 801(c) states: “Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, *offered in evidence to prove the truth of the matter asserted.*” (emphasis added). Thus, even if the evidence is an assertion, made by a declarant, it still is not hearsay unless offered to prove the truth of what is asserted. The advisory committee’s note to Rule 801(c) underscores this: “If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay. The effect is to exclude from hearsay the entire category of ‘verbal acts’ and ‘verbal parts of an act,’ in which the statement itself affects the legal rights of the parties or is a circumstance bearing on

conduct affecting their rights.” FED.R.EVID. 801(c) advisory committee’s note (citation omitted). *See also* WEINSTEIN at § 801.11[1] (“‘If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted.’ Thus, if a declarant’s statement is not offered for its truth, the declarant’s credibility is not material, and the statement is not hearsay.” (citation omitted)). Commentators have identified many instances in which assertive statements are not hearsay because they are not offered to prove the truth of the assertions: (1) statements offered to prove a claim that the statement was false or misleading, as in a fraud or misrepresentation case;<sup>FN42</sup> (2) statements offered to “prove that because they were made, listeners had notice or knowledge of the information related in the statements,” or to show the effect on the listener of the statement;<sup>FN43</sup> (3) statements “offered to prove an association\*566 between two or more persons;”<sup>FN44</sup> (4) statements offered as circumstantial evidence of the declarant’s state of mind,<sup>FN45</sup> or motive;<sup>FN46</sup> (5) statements that have relevance simply because they were made, regardless of their literal truth or falsity—the so called “verbal acts or parts of acts,”<sup>FN47</sup> also referred to as “legally operative facts”;<sup>FN48</sup> and (6) statements that are questions or imperative commands,<sup>FN49</sup> such as “what time is it” or “close the door.”

FN42. SALTZBURG at § 801.02[1][e].

FN43. *Id.* at § 801.02[1][f]; WEINSTEIN at § 801.11[5][a].

FN44. SALTZBURG at § 801.2[1][g]; *see also* WEINSTEIN at § 801.11[6].

FN45. SALTZBURG at § 801.02[1][h]. This category typically deals with statements from which the declarant’s state of mind is circumstantially inferred. For example, if someone says “Woe is me” it may be inferred

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

that they are depressed or sad. Such statements are in contrast to statements that constitute direct evidence of the declarant's state of mind, offered to prove that state of mind, for example "I feel good," offered to prove that the declarant felt good. The later example is hearsay, but covered by an exception, Rule 803(3): Then existing state of mind or condition.

FN46. WEINSTEIN at § 801.11[5][a], [c].

FN47. SALTZBURG at § 801.02[1][j].

FN48. WEINSTEIN at § 801.11[3]-[4].

FN49. *Id.* at § 801.11[2].

When analyzing the admissibility of electronically generated evidence, courts also have held that statements contained within such evidence fall outside the hearsay definition if offered for a purpose other than their substantive truth. *Siddiqui*, 235 F.3d at 1323 (e-mail between defendant and co-worker not hearsay because not offered to prove truth of substantive content, but instead to show that a relationship existed between defendant and co-worker, and that it was customary for them to communicate by e-mail); *Safavian*, 435 F.Supp.2d at 44 (e-mail from lobbyist to defendant not hearsay because they were not offered to prove their truth, but to illustrate the nature of the lobbyist's work on behalf of clients to provide context for other admissible e-mail; and as evidence of the defendant's intent, motive and state of mind); *Telewizja Polska USA*, 2004 WL 2367740; *Perfect 10*, 213 F.Supp.2d at 1155 (exhibits of defendant's website on a particular date were not "statements" for purposes of hearsay rule because they were offered to show trademark and copyright infringement, therefore they were relevant for a purpose other than their literal truth); *State v. Braidic*, 119 Wash.App. 1075, 2004 WL 52412 at \*1 (Jan. 13, 2004) (e-mail sent by de-

fendant to victim not hearsay because they were not offered to prove the truth of the statements.).

Finally, of particular relevance to this suit are the cases that have held that communications between the parties to a contract that define the terms of a contract, or prove its content, are not hearsay, as they are verbal acts or legally operative facts. *See, e.g., Preferred Properties Inc. v. Indian River Estates Inc.*, 276 F.3d 790, 799 n. 5 (6th Cir.2002) (verbal acts creating a contract are not hearsay); *Kepner-Tregoe, Inc. v. Leadership Software*, 12 F.3d 527, 540 (5th Cir.1994) (finding contract to be a signed writing of independent legal significance and therefore non-hearsay); *Mueller v. Abdnor*, 972 F.2d 931, 937 (8th Cir.1992) (holding contracts and letters from attorney relating to the formation thereof are non-hearsay); *United States v. Tann*, 425 F.Supp.2d 26, 29 (D.D.C.2006) (finding negotiable instruments to be legally operative documents that do not constitute hearsay); *Planmatics*, 137 F.Supp.2d at 621 (D.Md.2001) (holding testimony regarding instructions made to individuals is not hearsay because instructions were not statements of fact). *See also* WEINSTEIN at § 801.11[3].<sup>FN50</sup> Because the e-mails that the parties to this suit attached as unauthenticated exhibits to their summary judgment papers were introduced for the purpose of proving the making of the agreement to arbitrate the dispute regarding the damage caused by the lightning strike, and the terms of this agreement, \*567 they are not hearsay if offered for this purpose because they are verbal acts, or legally operative facts. What the parties did not do, however, was articulate the non-hearsay purpose for which the e-mails were offered; they merely attached them as exhibits, without further explanation of the purpose for which they were offered, or clarification that they were not offered for their substantive truth. Because evidence may be offered for more than one purpose, it may be relevant for its substantive truth, and potentially hearsay, or relevant for some other purpose, and non-hearsay. For this reason it is important for a party offering an exhibit into evidence to clearly explain each purpose for

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

which it is offered, and address any hearsay issues associated with each purpose for which it is offered.

FN50. A verbal act is an utterance of an operative fact that gives rise to legal consequences. Verbal acts, also known as statements of legal consequence, are not hearsay, because the statement is admitted merely to show that it was actually made, not to prove the truth of what was asserted in it. For example, the hearsay rule does not exclude relevant evidence as to what the contracting parties said or wrote with respect to the making or the terms of an agreement.

*Is the evidence excluded from the definition of hearsay by Rule 801(d)(1) or 801(d)(2).*

Once it has been determined whether evidence falls into the definition of hearsay because it is a statement, uttered by a declarant, and offered for its substantive truth, the final step in assessing whether it is hearsay is to see if it is excluded from the definition of hearsay by two rules: 801(d)(1), which identifies three types of prior statements by witnesses who actually testify and are subject to cross examination, which are excluded from the definition of hearsay, and 801(d)(2), which identifies five types of admissions by a party opponent that are excluded from the definition of hearsay. FED.R.EVID. 801(d) advisory committee's note ("[s]everal types of statements which would otherwise literally fall within the definition [of hearsay] are expressly excluded from it ..."); WEINSTEIN at § 801[20][1] & 801[30][1]; SALTZBURG at § 801.02[2] & 801.02[6].

Rule 801(d)(1) identifies three types of prior witness statements that are excluded from the definition of hearsay: first, 801(d)(1)(A) excludes prior inconsistent "testimonial statements" made under oath at a trial, hearing, court proceeding or deposition; next, 801(d)(1)(B) excludes prior consistent statements offered to rebut an express or implied allegation of recent fabrication, or improper influence or motive;

and finally, 801(d)(1)(C) excludes statements of identification of a person made after perceiving that person. For each of these exceptions, it is required that the declarant testify at trial and be subject to cross examination about the prior statements. FED. R. EVID. 801(d)(1); FED.R.EVID. 801(d)(1) advisory committee's note ("[Rule 801(d)(1)] requires in each instance, as a general safeguard, that the declarant actually testify as a witness, and it then enumerates three situations in which the statement is excepted from the category of hearsay."); WEINSTEIN at § 801.20[2] ("For a prior witness statement to escape the hearsay rule, the declarant must testify at trial and be subject to cross-examination concerning the statement." (citation omitted)).

Rule 801(d)(2) identifies five types of statements as "admissions by a party opponent," and excludes them from the definition of hearsay. Specifically: 801(d)(2)(A) excludes the party's own statement, made in either an individual or representative capacity; 801(d)(2)(B) addresses a statement by another that a party has adopted or manifested a belief in its truth; 801(d)(2)(C) deals with a statement by a person authorized by a party to make a statement concerning a subject; 801(d)(2)(D) excludes a statement made by a party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the agency or employment relationship; and 801(d)(2)(E) excludes the statement of a co-conspirator of a party made during the existence of the conspiracy and in furtherance of the conspiracy. To qualify as an admission, the party's out-of-court statement must be offered against that party, it cannot offer its own out of court statements as admissions. WEINSTEIN at § 801.30[1] ("To be admissible under [Rule 801(d)(2)], the party's statements must be offered *against* that party. A party cannot use this provision to offer his or her own statements into evidence.").

As can be seen from reading Rule 801(d)(1) and (2), there are specific foundational facts that must be

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

established before the statement or admission can be accepted into evidence. These determinations are made by the trial judge under Rule 104(a), and therefore the rules of evidence, except \*568 for privilege, are inapplicable. FED.R.EVID. 104(a), 1101(d)(1); FED.R.EVID. 104(a) advisory committee's note ("[W]hen a hearsay statement is offered as a declaration against interest, a decision must be made whether it possesses the required against-interest characteristics. These decisions too, are made by the judge.")

Given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party. *Siddiqui*, 235 F.3d at 1323 (ruling that e-mail authored by defendant was not hearsay because it was an admission under Rule 801(d)(2)(A)); *Safavian*, 435 F.Supp.2d at 43-44 (holding that e-mail sent by defendant himself was admissible as non-hearsay because it constituted an admission by the defendant, 801(d)(2)(A), and as an "adoptive admission" under Rule 801(d)(2)(B)); *Telewizja Polska USA*, 2004 WL 2367740 (N.D.Ill. Oct.15, 2004) (holding exhibits showing defendant's website as it appeared on a certain day were admissible as admissions against defendant); *Perfect 10*, 213 F.Supp.2d at 1155 (admitting e-mail sent by employees of defendant against the defendant as admissions under 801(d)(2)(D)).

If, after applying the foregoing four-step analysis, it is determined that the electronic evidence constitutes a statement by a person that is offered for its substantive truth and is not excluded from the definition of hearsay by Rule 801(d)(1) or (2), then the evidence is hearsay, and is inadmissible unless it qualifies as one of many hearsay exceptions identified by Rule 803, 804 and 807. The process of determining whether hearsay falls into one of the many exceptions can appear daunting, because there are twenty-three identified in Rule 803, five in Rule 804, and Rule 807,

the so-called "catch-all" exception, allows exceptions to be tailor made. Upon closer examination, however, the task is less onerous because the number of hearsay exceptions can be categorized in helpful ways that make them more manageable, and in most instances a handful of hearsay exceptions repeatedly are used in connection with electronically generated or stored evidence. Familiarity with these rules will suffice in most instances to overcome hearsay objections routinely made to ESI.

Rule 803 contains twenty-three separate hearsay exceptions. At first glance they may seem like they have nothing in common, but they do. All twenty-three are admissible regardless of whether the declarant is available to testify, distinguishing them from the five exceptions in Rule 804, each of which is inapplicable unless the declarant is "unavailable," as defined by any of the five methods identified in Rule 804(a). In addition, the twenty-three exceptions in Rule 803 may be grouped in three broad categories: **Category 1** includes exceptions dealing with **perceptions, observations, state of mind, intent and sensation** 803(1) (present sense impressions); 803(2) (excited utterances); 803(3) (then existing state of mind, condition or sensation); 803(4) (statements in furtherance of medical diagnosis and treatment). **Category 2** includes **documents, records, and other writings** 803(5) (past recollection recorded); 803(6) & (7) (business records); 803(8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12) (certificates of baptism, marriage and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) (ancient documents); 803(18) (learned treatises); 803(22) (judgments of conviction in a criminal case); and 803(23) (judgments in certain kinds of civil cases). **Category 3** includes statements dealing with **reputation** 803(19) (reputation regarding personal or family history); 803(20) (reputation regarding custom, use and practice associated with land, and historically

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

significant facts); and 803(21) (reputation regarding character within the community and among associates).

Given the widely accepted fact that most writings today are created and stored in electronic format, it is easy to see that the many types of documents and writings covered in Rule 803 will implicate electronic writings. Similarly, given the ubiquity of communications in electronic media (e-mail, \*569 text messages, chat rooms, internet postings on servers like “myspace” or “youtube” or on blogs, voice mail, etc.), it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium. It would unnecessarily prolong an already lengthy opinion to analyze all of the implications of the hearsay exceptions in Rule 803 as they relate to ESI. It is possible, however, to focus on the handful that have been discussed by the courts and that are most likely to be used in a hearsay analysis of ESI. Because the court's research has shown that the Rule 803 hearsay exceptions, rather than those found in Rules 804 or 807, have been cited by courts evaluating the hearsay implications of electronic evidence, the following analysis will be confined to that rule.

#### *Rule 803(1) Present Sense Impression*

Rule 803(1) creates an exception from exclusion under the hearsay rule for:

“(1) Present sense impression. A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.”

There are three elements that must be met for this hearsay exception to apply: (1) the declarant must have personally perceived the event that is described in the statement; (2) the statement must be a simple

explanation or description of the event perceived; and (3) the declaration and the event described must be contemporaneous. WEINSTEIN at § 803.03[1]. Present sense impressions are considered trustworthy because the near simultaneous expression of the explanation or description of the event with its perception militates against any memory deficiency, or opportunity to intentionally misstate what occurred. FED.R.EVID. 803(1) advisory committee's note (“The underlying theory of Exception (1) is that substantial contemporaneity of event and statement negate the likelihood of deliberate or conscious misrepresentation.”); WEINSTEIN at § 803.03[1].

#### *Rule 803(2) Excited Utterance*

Closely related to Rule 803(1) is Rule 803(2),<sup>FN51</sup> the excited utterance exception to the hearsay rule, which provides:

FN51. See FED.R.EVID. 803(1)-(2) advisory committee's note (“Exceptions (1) and (2) [to Rule 803]. In considerable measure these two examples overlap, though based on somewhat different theories. The most significant practical difference will lie in the time lapse allowable between the event and statement.”).

“(2) Excited utterance. A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.”

The theory behind the excited utterance exception is that perception of a startling or exciting event produces in the declarant an emotional state that reduces the likelihood that the description of the event while under this emotional state will be inaccurate or purposely misstated. FED.R.EVID. 803(2) advisory committee's note (“The theory of Exception (2) is simply that circumstances may produce a condition of excitement which temporarily stills the capacity of reflection and produces utterances free of conscious fabrication.”); WEINSTEIN at §

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

803.04[1] (“The premise underlying the exception for excited utterances is that a person under the influence of excitement precipitated by an external startling event will not have the reflective capacity essential for fabrication.”).

The prevalence of electronic communication devices, and the fact that many are portable and small, means that people always seem to have their laptops, PDA's, and cell phones with them, and available for use to send e-mails or text messages describing events as they are happening. Further, it is a common experience these days to talk to someone on the phone and hear them typing notes of the conversation on a computer as you are talking to them. For these reasons, Rules 803(1) and (2) may provide hearsay exceptions for electronically stored communications containing either present sense impressions or excited utterances. *See, e.g., United States v. Ferber*, 966 F.Supp. 90 (D.Mass.1997) (holding that e-mail from employee to boss about substance of telephone call with defendant in mail/wire fraud case \*570 did qualify as a present sense expression under Rule 803(1), but did not qualify as an excited utterance under Rule 803(2), despite the language at the end of the e-mail “my mind is mush.”); *State of New York v. Microsoft*, 2002 WL 649951 (D.D.C. Apr.12, 2002) (analyzing the admissibility of series of exhibits including e-mail and e-mail “chains” under various hearsay exceptions, and ruling that an e-mail prepared several days after a telephone call that described the call did not qualify as a present sense impression under Rule 803(1) because the requirement of “contemporaneity” was not met).

#### ***Rule 803(3) Then Existing State of Mind or Condition***

Rule 803(3) provides a hearsay exception for:

“(3) Then existing mental, emotional, or physical condition. A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design,

mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will.”

Rule 803(3) also is closely related to Rule 803(1). *See* FED.R.EVID. 803(3) advisory committee's note (“Exception (3) [to Rule 803] is essentially a specialized application of Exception (1), presented separately to enhance its usefulness and accessibility.”). The rule permits the statement of the declarant's state of mind, sensation, mental, emotional, or physical condition, as well as statements of motive, intent, plan or design, but excludes statements of memory or belief if offered to prove the truth of the fact remembered. FED.R.EVID. 803(3) advisory committee's note (“The exclusion of ‘statements of memory or belief to prove the fact remembered or believed’ is necessary to avoid the virtual destruction of the hearsay rule which would otherwise result from allowing state of mind, provable by a hearsay statement, to serve as the basis for an inference of the happening of the event which produced the state of mind.”). The foundation for proving an exception under Rule 803(3) is: (1) The statement must be contemporaneous with the mental state being proven; (2) There must be [an absence of] suspicious circumstances that would evidence a motive for fabrication or misrepresentation of the declarant's state of mind; and (3) The state of mind of the declarant must be relevant in the case. WEINSTEIN at § 803.05[2][a]. Rule 803(3) has been used to prove a wide variety of matters, including the reason why the declarant would not deal with a supplier or dealer, motive, competency, ill-will, motive, lack of intent to defraud, willingness to engage in criminal conduct, the victim's state of mind in an extortion case, and confusion or secondary meaning in a trademark infringement case. *Id.*

Rule 803(3) is particularly useful when trying to admit e-mail, a medium of communication that seems particularly prone to candid, perhaps too-candid,

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

statements of the declarant's state of mind, feelings, emotions, and motives. Indeed, courts have analyzed this rule in connection with ruling on the admissibility of electronic evidence. In *New York v. Microsoft*, the court analyzed admissibility of e-mail and e-mail chains under a variety of hearsay rules, including 803(3). 2002 WL 649951. It concluded that an e-mail made several days following a telephone conversation did not qualify under Rule 803(3) because it contained more than just the declarant's state of mind, but also included the maker's memory of belief about the events that affected his state of mind, which is specifically excluded by Rule 803(3). *Id.* at \*5. See also *Safavian*, 435 F.Supp.2d at 44 (admitting e-mail that contained statements of defendant's state of mind under Rule 803(3)).

#### **Rule 803(6) Business Records**

Rule 803(6) recognizes an exception to the hearsay rule for:

“(6) Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business \*571 activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term ‘business’ as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.”

The foundational elements for a business record are: (1) The document must have been prepared in the normal course of business; (2) it must have been made

at or near the time of the events it records; (3) it must be based on the personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant;<sup>FN52</sup> and (4) to have been made in the normal course of business means that the document was made in the regular course of a regularly conducted business activity, for which it was the regular practice of the business to maintain a memorandum. WEINSTEIN at § 803.08[1]. 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 e-mail.

FN52. The majority view is that the source of the information memorialized in the business record must have a business duty to transmit the information to the maker of the record, if the maker him or herself lacks personal knowledge of the facts or events. See, e.g., FED.R.EVID. 803(3) advisory committee's note (“Sources of information presented no substantial problem with ordinary business records. All participants, including the observer or participant furnishing the information to be recorded, were acting routinely, under a duty of accuracy, with the employer reliance on the result, or in short ‘in the regular course of business’. If, however, the supplier of the information does not act in the regular course, an essential link is broken; the assurance of accuracy does not extend to the information itself, and the fact that it may be recorded with scrupulous accuracy is of no avail.”). However, some courts have held that it may be possible to meet the requirements of the business record exception even if the source of the information had no business duty to provide it to the maker of the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

record, provided the recipient of the information has a business duty to verify the accuracy of the information provided. *See, e.g., Rambus*, 348 F.Supp.2d at 706-07 (Court noted that ordinarily, when the supplier of the information recorded in the business record does not act in the regular course of the business, an “essential link” in the foundation is broken, but recognized that “[w]hen the source of the information in the business record is an outsider, the only way to save the record from the jaws of the hearsay exclusion is to establish that the business recipient took precautions to guarantee the accuracy of the given information. Thus, the company must have been able in some way to verify the information provided.” (citation omitted)).

Rule 902(11) also is helpful in establishing the foundation elements for a business record without the need to call a sponsoring witness to authenticate the document and establish the elements of the hearsay exception. Rule 902(11) permits the self-authentication of a business record by showing the following:

“(11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record-

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly con-

ducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.”

**\*572** Because the elements for both rules are essentially identical, they frequently are analyzed together when Rule 902(11) is the proffered means by which a party seek to admit a business record. *See In re Vee Vinhnee*, 336 B.R. at 446; *Rambus*, 348 F.Supp.2d at 701 (holding that analysis of Rule 803(6) and 902(11) go “hand in hand,” and identifying the following requirements for authentication under Rule 902(11):(1) a qualified custodian or other person having personal knowledge makes the authenticating declaration, who must have “sufficient knowledge of the record-keeping system and the creation of the contested record to establish their trustworthiness;” (2) the declaration must establish that the record was made at or near the time of the occurrence or matters set forth in the document by someone with personal knowledge of these matters or from information provided by someone with personal knowledge thereof; (3) the declaration must show that the record is kept in the course of the regularly conducted activity of the business, and the “mere presence of a document ... in the retained file of a business entity do[es] not by itself qualify as a record of a regularly conducted activity”; and (4) the declaration must establish that it is the regular practice of the business to keep records of a regularly conducted activity of the business, and “it is not enough if it is the regular practice of an employee to maintain the record of the regularly conducted activity .... it must be the regular practice of the business entity to do so”-i.e. it is at the direction of the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

company that the employee maintain the record).

The business record exception is one of the hearsay exceptions most discussed by courts when ruling on the admissibility of electronic evidence. The decisions demonstrate a continuum running from cases where the court was very lenient in admitting electronic business records, without demanding analysis, to those in which the court took a very demanding approach and scrupulously analyzed every element of the exception, and excluded evidence when all were not met. For example, in *State of New York v. Microsoft*, the court analyzed the admissibility of “e-mail chains.” 2002 WL 649951 (D.D.C. Apr.12, 2002). The court held that an e-mail prepared by an employee did not qualify as a business record because, while it may have been the regular practice of the employee to send an e-mail following the receipt of a phone call that summarized the call, there had been no showing that it was the regular practice of the employer to require that the employee make and maintain such e-mails. *Id.* at \*9. The court was particularly careful in analyzing the hearsay issues associated with e-mail chains involving multiple employees of the same employer. It held that to establish a proper foundation, the proponent would have to show that when the source of the information related in the e-mail is someone other than the maker of the e-mail, that the source, the maker “as well as every other participant in the chain producing the record are, acting in the regular course of [the] business.” *Id.* at \*14. If this showing is made, the court ruled, then the multiple levels of hearsay in the e-mail chain are covered by Rule 803(6). However, “[i]f the source of the information is an outsider, Rule 803(6) does not, by itself, permit the admission of the business record. The outsider’s statement must fall within another hearsay exception to be admissible because it does not have the presumption of accuracy that statements made during the regular course of business have.” *Id.* at \*14. The court also excluded another e-mail chain for failure of the proponent to establish a proper foundation, saying “[p]laintiffs have not established the req-

uisite foundation that the multiple authors of these e-mails each composed their portion of the document in the course of regularly conducted business activity and that it was the regular practice of RealNetworks to compose such e-mail correspondence. Moreover, the multiple authors and forwarded nature of the e-mails undercuts the reliability of the information contained therein.” *Id.* at \*19.

Similarly, in *Rambus Inc. v. Infineon Tech. AG*, the Court critically analyzed the admissibility of e-mail under the business record exception to the hearsay rule. 348 F.Supp.2d 698, 706 (E.D.Va.2004). Certain exhibits objected to by the defendant were e-mail chains prepared at least in part by persons outside of the business entity that maintained the e-mail as part of its records, and which was seeking their admissibility as \*573 business records. The court noted that there was “not a requirement that the records have been prepared by the entity that has custody of them, as long as they were created in the regular course of some [other] entity’s business.” *Id.* (quoting WEINSTEIN, at § 803.08[8][a]). The court added “[h]owever, it also is true that: To satisfy Rule 803(6) each participant in the chain which created the record-from the initial observer-reporter to the final entrant-must generally be acting in the course of the regularly conduct[ed] business. *Id.* at 707. If some participant is not so engaged, some other hearsay exception must apply to that link of the chain.” *Id.* at 706.

In contrast to the demanding approach taken in *Rambus* and *New York v. Microsoft*, the court in *United States v. Safavian* took a more flexible approach to the admissibility of e-mail chains. 435 F.Supp.2d 36, 40-41 (D.D.C.2006). The defendant objected to the admissibility of e-mail chains, arguing that they were not trustworthy because they contained e-mails embedded within e-mails. The court overruled this objection, stating:

“[t]he defendant’s argument is more appropriately

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

directed to the weight the jury should give the evidence, not its authenticity. While the defendant is correct that earlier e-mails that are included in a chain-either as ones that have been forwarded or to which another has replied-may be altered, this trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice.... The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course.... We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of the nation's population and is of particular importance in the professional world.... Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done."

*Id.* at 41. Notably, the court did not engage in the demanding business records exception analysis that was done by the courts in *Rambus and New York v. Microsoft*.

Perhaps the most demanding analysis regarding the admissibility of electronic evidence under the business record exception to the hearsay rule appears in *In re Vee Vinhnee*, 336 B.R. at 445. In this case the appellate bankruptcy panel upheld the trial bankruptcy judge's exclusion of electronic business records, observing that "early versions of computer foundations [accepted by courts] were too cursory, even though the basic elements [of the business records exception] covered the ground." The court held that the proponent of an electronic business record was required to show that the paperless electronic record retrieved from its computer files was the same one as originally had been entered into its computer, noting that 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 cre-

ated." *Id.* at 444. It added "[t]he logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the questions of whether records have been changed since their creation." *Id.* at 445. The court reasoned that the "complexity of ever-developing computer technology necessitates more precise focus," because "digital technology makes it easier to alter text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to assure the continuing integrity of the records." *Id.*

In contrast to the demanding approach taken in *In re Vee Vinhnee*, many other courts have admitted electronic business records\*574 under a much more relaxed standard. See, e.g., *United States v. Kassimu*, 2006 WL 1880335 (5th Cir.2006) (Establishing the foundation for a computer generated business record did not require the maker of the record, or even a custodian, but only a witness qualified to explain the record keeping system of organization.); *United States v. Fujii*, 301 F.3d 535 (7th Cir.2002) (holding that computerized check-in and reservation records were admissible as business records on a showing that the data reflected in the printouts was kept in the ordinary course of the business); *Sea-Land*, 285 F.3d 808 (holding that copy of electronic bill of lading had been properly admitted as a business record because it had been produced from the same electronic information that had been contemporaneously generated when the parties entered into their contract. The court noted that "it is immaterial that the business record is maintained in a computer rather than in company books." (citation omitted)); *Wapnick v. Commissioner of Internal*

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

*Revenue*, T.C. Memo.2002-45, 2002 WL 215993 (T.C.2002)(computerized accounting records were admissible as business records because foundation was established by IRS agents who compared the data in the computer records with information in the company's tax returns, bank statements, and by contacting clients of the company to verify information in the computerized records).

The lesson to be taken from these cases is that some courts will require the proponent of electronic business records or e-mail evidence to make an enhanced showing in addition to meeting each element of the business records exception. These courts are concerned that the information generated for use in litigation may have been altered, changed or manipulated after its initial input, or that the programs and procedures used to create and maintain the records are not reliable or accurate. Others will be content to view electronic business records in the same light as traditional "hard copy" records, and require only a rudimentary foundation. Unless counsel knows what level of scrutiny will be required, it would be prudent to analyze electronic business records that are essential to his or her case by the most demanding standard. The cases further suggest that during pretrial discovery counsel should determine whether opposing counsel will object to admissibility of critical documents. This can be done by requesting a stipulation, or by propounding requests for admission of fact and genuineness of records under FED.R.CIV.P. 36. If it is known that opposing counsel will object, or refuses to stipulate, or denies a Rule 36 request to admit genuineness, then the lawyer intending to introduce the electronic business record should be prepared to establish the business record exception under the most demanding standard required, to avoid exclusion of the evidence.

#### **Rule 803(8) Public Records.**

In addition to the above described hearsay exceptions, courts have found that electronic records also met the requirements of the public records ex-

ception under Rule 803(8):

"(8) Public records and reports. Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness."

Furthermore, "[j]ustification for the exception is the assumption that a public official will perform his duty properly, and the unlikelihood that he will remember details independently of the record." FED.R.EVID. 803(8) advisory committee's note. Moreover, "[s]ince the assurances of accuracy are generally greater for public records than for regular business records, the proponent is usually not required to establish their admissibility through foundation testimony.... The burden of proof concerning the admissibility of public records is on the party opposing their introduction." WEINSTEIN at § 803.10[2]. Courts have applied this deferential standard of admissibility for electronic \*575 public records. *See, e.g., EEOC v. E.I. DuPont de Nemours and Co.*, 2004 WL 2347556 (holding that table of information compiled by U.S. Census Bureau was admissible as an exception to the hearsay rule as a public record under Rule 803(8), and rejecting claims that the posting of data on the Census Bureau's website rendered it untrustworthy); *Lester v. Natsios*, 290 F.Supp.2d 11 (D.D.C.2003) (admitting e-mail of public agency, and noting that "[r]ecords of public agencies such as those challenged by plaintiff are generally admissible ... under FED.R.EVID. 803(8)."); *United States v. Oceguedra-Aguirre*, 70 Fed.Appx. 473 (9th Cir.2003)

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

(Court held that trial court properly admitted computerized records of Treasury Enforcement Communications System as public records under Rule 803(8) because documents falling under the public records exception are presumed to be trustworthy, and the burden is on the party challenging the records to establish untrustworthiness.)

***Rule 803(17) Market Reports, Commercial Publications.***

Rule 803(17) recognizes as an exception to the hearsay rule:

“(17) Market reports, commercial publications. Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations.”

This exception covers “lists, etc., prepared for the use of a trade or profession ... newspaper market reports, telephone directories, and city directories. The basis of trustworthiness is general reliance by the public or by a particular segment of it, and the motivation of the compiler to foster reliance by being accurate.” FED.R.EVID. 803(17) advisory committee’s note; WEINSTEIN at § 803. 19[1].<sup>FN53</sup> At least one court has admitted electronically stored compilations and directories under Rule 803(17). *Elliott Assoc. L.P. v. Banco de la Nacion*, 194 F.R.D. 116, 121 (S.D.N.Y.2000) (finding that plaintiff’s expert report properly relied on prime rates of interest obtained from Federal Reserve Board website because they were reliable under Rule 803(17)).

FN53. “[T]he admissibility of market reports and commercial publications under Rule 803(17) is predicated on the two factors of necessity and reliability. Necessity lies in the fact that if this evidence is to be obtained it must come from the compilation, since the task of finding every person who had a hand

in making the report or list would be impossible. Reliability is assured because the compilers know that their work will be consulted; if it is inaccurate, the public or the trade will cease consulting their product.” (citation omitted).

A final observation needs to be made regarding hearsay exceptions and electronic evidence. Rule 802 generally prohibits the admission of hearsay unless one of the exceptions in Rules 803, 804 or 807 apply. What, then, is the effect of hearsay evidence that is admitted without objection by the party against whom it is offered? The general rule is that despite Rule 802, if hearsay is admitted without objection it may be afforded its “natural probative effect, as if it were in law admissible.” *New York v. Microsoft*, 2002 WL 649951 (“[I]n this country the general rule supported by overwhelming weight of authority is that where ordinarily inadmissible hearsay evidence is admitted into evidence without objection it may properly be considered and accorded its natural probative effect, as if it were in law admissible.”); 3 MICHAEL H. GRAHAM, HANDBOOK OF FEDERAL EVIDENCE § 802.1 (5th ed. 2001) (“In the absence of an objection to hearsay ‘the jury may consider [the hearsay] for whatever natural value it may have; such evidence is to be given its natural probative effect as if it were in law admissible.’ ” (citation omitted)). This underscores the need to pay attention to exhibits offered by an opponent, as much as to those records that you need to introduce. A failure to raise a hearsay objection means that the evidence may be considered for whatever probative value the finder of fact chooses to give it.

In summary, when analyzing the admissibility of ESI for hearsay issues, counsel should address each step of the inquiry in order: does the evidence contain a statement, made by a person, which is offered for its substantive truth, but which does not fall into the two categories of statements identified in 801(d)(1) and 801(d)(2). If, as a result of this analysis, a determina-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

tion is made that \*576 the evidence is hearsay, then it is inadmissible unless it covered by one of the exceptions found in Rules 803, 804 and 807.

If ESI has cleared the first three hurdles by being shown to be relevant, authentic, and admissible under the hearsay rule or an exception thereto, it must also be admissible under the original writing rule before it can be admitted into evidence or considered at summary judgment.

#### *The Original Writing Rule, Rules 1001-1008*

The next step in evaluating the admissibility of electronic evidence is to analyze issues associated with the original writing rule, which requires an original or duplicate original to prove the contents of a writing, recording or photograph unless secondary evidence is deemed acceptable.<sup>FN54</sup> See FED.R.EVID. 1001-08. The best way to understand the rule is to appreciate its structure. Rule 1001 contains the key definitions that animate the rule: “original,” “duplicate,” “writing,” “recording,” and “photograph.” The substantive requirements of the original writing rule are succinctly provided by Rule 1002, which mandates that “[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.” It is Rule 1002 that gives the rule its modern name, the “original writing rule,” as it requires the original to prove the contents of a writing, recording or photograph, except as excused by the remaining rules in Article X of the rules of evidence. As will be seen, the key to the rule is to determine when “the contents” of a writing, recording or photograph actually are being proved, as opposed to proving events that just happen to have been recorded or photographed, or those which can be proved by eyewitnesses, as opposed to a writing or recording explaining or depicting them. Rule 1003 essentially provides 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. *People v. Huehn*, 53 P.3d 733, 738 (Colo.Ct.App.2002) (duplicates of computer generated bank records admissible to the same extent as an original absent unfairness or lack of authenticity). Because of Rule 1003, duplicates are more often admitted into evidence than originals. RICE at 192 (“As a practical matter, Fed.R.Evid. 1003 has eliminated best evidence objections. Copies from the pages of books, treatises, and the other papers are now introduced in place of the entire volume because photocopies of originals are now admissible as if they were the original.”). Rule 1004 is the primary rule that identifies when secondary evidence is admissible. As a practical matter, “secondary evidence” is any proof of the contents of a writing, recording or photograph other than an original or duplicate. Examples include testimony from the author of the writing, or someone who read it, earlier drafts, copies, or an outline used to prepare the final. Rule 1005 describes how to prove the contents of public records, since it is obvious that something other than the original must be used. Rule 1006 permits introduction into evidence of written or testimonial summaries of voluminous writings, recordings or photographs, provided the original or duplicates from which the summaries were prepared were made available to the adverse party at a reasonable time in advance of trial for examination or copying. Thus, Rule 1006 is an example of secondary evidence. Rule 1007 allows the proof of the contents of a writing, recording or photograph by the deposition or testimony of a party opponent, without having to account for the nonproduction of the original. This is another form of secondary \*577 evidence. The final rule in Article X of the Federal Rules of Evidence is Rule 1008. It is a specialized application of Rule 104(b)-the conditional relevance rule-and sets forth what must happen when there is a dispute regarding whether there ever was a writing, recording, or photograph, or when there are conflicting versions of duplicates, originals, or secondary evidence offered into evidence. In such instances, as in Rule 104(b), the jury decides the factual dispute. FED.R.EVID. 1008 advisory committee's note.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

FN54. Traditionally the rule has been referred to as the “Best Evidence Rule,” which is a misleading title. The rule is more accurately is referred to as the “Original Writing Rule” because it does not mandate introduction of the “best” evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an “original,” “duplicate” or, in certain instances, by “secondary evidence”—any evidence that is something other than an original or duplicate (such as “testimony, or a draft of a writing to prove the final version, if no original or duplicate is available.”) FED.R.EVID. 1001 advisory committee’s note; RICE at 190 (“Article X of the Federal Rules of Evidence codified the common law best evidence rule, terming it instead the original writing rule.”).

It has been acknowledged that the original writing rule has particular applicability to electronically prepared or stored writings, recordings or photographs. One respected commentator has observed:

“Computer-based business records commonly consist of material originally produced in a computer (e.g. business memoranda), data drawn from outside sources and input into the computer (e.g. invoices), or summaries of documents (e.g. statistical runs). The admissibility of computer-based records ‘to prove the content of a writing’ is subject to the best evidence rule set out in Rule 1002. The rule generally requires the original of a writing when the contents are at issue, except that a ‘duplicate’ is also admissible unless a genuine issue is raised about its authenticity. A duplicate includes a counterpart produced by ‘electronic re-recording, which accurately reproduces the original.’ Courts often admit computer-based records without making the distinction between originals and duplicates.”

WEINSTEIN at § 900.07[1][d][iv] (citation omitted).

When analyzing the original writing rule as it applies to electronic evidence, the most important rules are Rule 1001, containing the definitions; Rule 1002, the substantive original writing rule; Rule 1004, the “primary” secondary evidence rule; Rule 1006, the rule permitting summaries to prove the contents of voluminous writings, recordings and photographs; and Rule 1007, allowing proof of a writing, recording or photograph by the admission of a party opponent.

Rule 1001 states:

“For purposes of this article the following definitions are applicable:

- (1) Writings and recordings. “Writings” and “recordings” consist of letters, words, or numbers, or their equivalent, set down by handwriting, type-writing, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.
- (2) Photographs. “Photographs” include still photographs, X-ray films, video tapes, and motion pictures.
- (3) Original. An “original” of a writing or recording is 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.”
- (4) Duplicate. A “duplicate” is 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 me-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

chanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.”

It is apparent that the definition of “writings, recordings and photographs” includes evidence that is electronically generated and stored. *See* FED. RULE EVID. 1001 advisory committee's note (“Traditionally the rule requiring the original centered upon accumulations of data and expressions affecting legal relations set forth in words and figures. This meant that the rule was one essentially related to writings. Present day techniques have expanded methods of storing data, yet the essential form that the information ultimately assumes for useable purposes is words and figures. Hence, the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments.”). It further is clear that under Rule 1001(3) the “original” of information stored in a computer is the readable display of the information on the computer screen, the hard drive or \*578 other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data. WEINSTEIN at § 900.07 [1][d][iv]; RICE at 194; *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind.Ct.App.2002) (ruling that content of internet chat room communications between defendant and undercover police officer that officer “cut-and-pasted” into a word processing program were originals under state version of original writing rule). Moreover, if a computer record accurately reflects the contents of another writing, and was prepared near the time that the original writing was prepared, it may qualify as an original under Rule 1001. *In re Gulph Woods Corp.*, 82 B.R. 373, 377 (Bankr.E.D.Pa.1988) <sup>FN55</sup>. *See also* WEINSTEIN at § 900.07[1][d][iv]. Finally, as already noted, as a result of Rule 1003, the distinction between duplicates and originals largely has become unimportant, as duplicates are co-extensively admissible as originals in most instances.

FN55. “In today's commercial world, a single

transaction often generates successive entries of the same information in separately prepared writings. Though the purposes of these separate records may be different, a computerized business record, prepared simultaneously with or within a reasonable time period of the written record, and containing the same or similar information, would appear to be no less an ‘original’ than a handwritten record. However, it seems equally clear that where a written record, prepared prior to the computer record, contains a more detailed and complete description of the transaction than that contained in the computer record, the proponent of the evidence should be required to produce the more detailed record, or account for its nonproduction under F.R.E. 1004. Similarly, where a computerized record appears to be nothing more than a summary of a more detailed written record, the written record should be produced except where the requirements of F.R.E. 1006 have been satisfied.” (citations omitted).

Once the definitions of the original writing rule are understood, the next important determination is whether the rule applies at all. Rule 1002 answers this question. It provides: “To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.” As the advisory committee's note to Rule 1002 makes clear:

“Application of the rule requires resolution of the question whether contents are sought to be proved. Thus an event may be proved by non-documentary evidence, even though a written record of it was made. If, however, the event is sought to be proved by the written record, the rule applies. For example, payment may be proved without producing the written receipt which was given. Earnings may be

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

proved without producing books of account in which they are entered. Nor does the rule apply to testimony that books or records have been examined and found not to contain any reference to a designated matter.

The assumption should not be made that the rule will come into operation on every occasion when use is made of a photograph in evidence. On the contrary, the rule will seldom apply to ordinary photographs.... On occasion, however, situations arise in which contents are sought to be proved. Copyright, defamation, and invasion of privacy by photograph or motion picture falls into this category. Similarly, as to situations in which the picture is offered as having independent probative value, e.g. automatic photograph of bank robber, photograph of defendant engaged in indecent act.”

FED.R.EVID. 1002, advisory committee's note (citations omitted); *see also* WEINSTEIN at § 1002.05[1] (“The best evidence rule only applies when the writing, recording or photograph is being introduced ‘to prove the content of a writing, recording or photograph’. The rule is inapplicable when content is not at issue.”)(citing FED.R.EVID. 1002). Whether the content is at issue is determined on a case-by-case basis. *Id.* For example, proof that someone is married may be made by the testimony of a witness to the ceremony. The marriage license is not required. However, the rule applies if the only proof of the marriage is by the record itself. Similarly, someone who heard a politician give a speech may testify to what was said without the video recording of the speech, because the content of the recording is not at issue. In contrast, if the only way to prove the content of the speech is by the video, because there \*579 are no witnesses available to testify, the rule would apply to the video recording.

Rule 1002 also does not apply when an expert testifies based in part on having reviewed writings, recordings or photographs, because Rule 703 allows

an expert to express opinions based on matters not put into evidence. FED.R.EVID. 1002 advisory committee's note; WEINSTEIN at § 1002.05[1] (“The best evidence rule does not apply when an expert resorts to material as a basis for an opinion.”). Finally, when the contents of writings, recordings or photographs merely are collateral to the case, meaning they are not “closely related to a controlling issue” in a case, Rule 1002 does not apply, and secondary evidence may be used to prove their contents. FED.R.EVID. 1004(4). In contrast, proving legal transactions, such as wills, contracts, and deeds commonly do involve the best evidence rule because the documents themselves have the central legal significance in the case. WEINSTEIN at § 1002.05[2].

An example of when the original writing rule did apply to electronic evidence is *Laughner v. State*, 769 N.E.2d 1147 (Ind.Ct.App.2002), *abrogated on other grounds by Fajardo v. State*, 859 N.E.2d 1201 (Ind.2007). Laughner was charged with attempted child solicitation. To prove the crime, the state offered printouts of instant message chats between the defendant and an undercover police officer posing as a thirteen year old boy. The police officer “cut-and-pasted” the text of the text messages from the internet chat room into a word processing program, and the printouts that were introduced into evidence were prepared from that program. The defendant objected (citing the state version of the original writing rule, which was identical to the federal version), arguing that the printouts were not the “original” of the text of the chat room communications. The appellate court agreed that the state was proving the content of a writing, and that the original writing rule required an original, but found that the printout was an original, reasoning:

“Evidence Rule 1002, the ‘best evidence’ rule, requires an ‘original’ in order to prove ‘the content’ of a writing or recording. However, Evidence Rule 1001(3) provides that when ‘data are stored in a computer or similar device, any printout or other

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

output readable by sight, shown to reflect the data accurately is an 'original.' According to [the police officer] he saved the conversations with Laughner after they were concluded, and the printout document accurately reflected the content of those conversations. Therefore, the printouts could be found to be the 'best evidence' of the conversations [between the defendant and the officer]."

*Laughner*, 769 N.E.2d at 1159.

It is important to keep in mind that failure to properly object to the introduction of evidence in violation of the original writing rule likely will result in a waiver of the error on appeal. WEINSTEIN at § 1002.04[5][a] ("Procedural safeguards adopted by federal courts also militate against an overtechnical application of the best evidence rule. For example, an appellant's failure to properly raise an objection to the best evidence rule at trial will result in waiver of the error on appeal."); see also *State v. Braidic*, 119 Wash.App. 1075, 2004 WL 52412 (2004) (Defendant was convicted of rape and other sex offenses with minor. At trial, victim's mother testified, without objection, to content of chat room text messages between defendant and victim. Appellate court noted applicability of original writing rule to require original to prove the contents of the chat room records, but found that defense counsel's failure to object did not constitute ineffective assistance of counsel). Counsel need to insure that a timely objection is made to attempts to prove the contents of electronic writings, recordings or photographs in violation of the original writing rule, otherwise waiver of the error is the probable consequence.

Rule 1004 identifies four circumstances in which secondary evidence may be introduced instead of an original. The rule provides:

"The original is not required, and other evidence of the contents of a writing, recording, or photograph

is admissible if-

(1) Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or

\*580 (2) Original not obtainable. No original can be obtained by any available judicial process or procedure; or

(3) Original in possession of opponent. At a time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing; or

(4) Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue."

The first example may be particularly suited for electronic evidence. Given the myriad ways that electronic records may be deleted, lost as a result of system malfunctions, purged as a result of routine electronic records management software (such as the automatic deletion of e-mail after a set time period) or otherwise unavailable means that the contents of electronic writings may have to be proved by secondary evidence.<sup>FN56</sup> Indeed, at least one court has recognized that the "tenuous and ethereal nature of writings posted in internet chat rooms and message boards means that in all likelihood the exceptions [to the original writing rule that permit secondary evidence] would ... [apply]." *Bidbay.com, Inc. v. Spry*, 2003 WL 723297 (Cal.App.2003)(unpublished opinion); *People v. Huehn*, 53 P.3d 733, 738 (Colo.Ct.App.2002) (holding that trial court did not abuse discretion in admitting computer generated bank records that contained listing of ATM transactions prepared by another company that bank retained to process ATM transactions. The court noted that the Col-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

orado version of Rule 1004(1) permitted secondary evidence of the records provided they were not lost or destroyed in bad faith).

FN56. *See*, for example, newly revised Fed.R.Civ.P. 37(f), which creates a limited “safe harbor” from sanctions if electronically stored information is not preserved as a result of the routine good faith operation of an electronic records management system. Sanctions may be imposed if the court finds the presence of “extraordinary circumstances” or if it determines that the loss of the ESI was the result of non-routine loss or destruction, or action taken in the absence of good faith. The new rule evidences the widespread recognition that electronically stored information is not infrequently lost or destroyed.

Additionally, Rule 1004 permits proof of the contents of a writing, recording or photograph by secondary evidence when the proponent of the evidence is unable to obtain an original through use of legal process, or when the original is in the possession or control of an adverse party that has actual or inquiry notice of the contents that the proponent intends to introduce the evidence. In the later circumstance, as the advisory committee's note to Rule 104(3) points out, “[a] party who has an original in his control has no need for the protection of the [original writing] rule if put on notice that proof of contents will be made. He can ward off secondary evidence by offering the original.”

Finally, Rule 1004(4) permits proof of the contents of writings, recordings or photographs by secondary evidence if they relate to “collateral matters,” defined as “not closely related to a controlling issue” in the case. The advisory committee's note to Rule 1004(4) candidly acknowledges that this is a nebulous standard, stating “[w]hile difficult to define with precision, situations arise in which no good purpose is served by production of the original.” *See also*

WEINSTEIN at § 1004.40 (“[t]he distinction between controlling and collateral issues can be an exasperating one. The term ‘collateral’ is elusive and vague. It cannot be defined conceptually, only pragmatically: balancing the importance of the document against the inconvenience of compelling its production, is the rule worth enforcing?”) (citation omitted). An example illustrates. A doctor testifying as an expert in a personal injury case can testify that she is licensed to practice medicine in a state without having to produce the license itself. However, if a defendant is charged with practicing medicine without a license, his testimony alone that he has a license from the state will not be accepted, as the license is closely related to a controlling issue in the case.

Rule 1006 recognizes another source of secondary evidence to prove the contents of writings, recordings, or photographs, stating:

**\*581** “The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.”

The advisory committee's note recognizes that Rule 1006 is one of necessity, as the “admission of summary of voluminous books, records, or documents offers the only practicable means of making their contents available to judge and jury.” A number of observations may be made about the use of summaries under Rule 1006. First, as the rule expressly states, the writings, recordings or photographs to be summarized must be voluminous. WEINSTEIN at § 1006.03 (“Charts, summaries or calculations are, however, inadmissible when the content being proved is neither voluminous or complicated.”) (citations omitted). Second, although the rule is silent on the nature of the summary, the prevailing view is that it may be either

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

written, or testimonial. *Id.* at § 1006.05[2] (“[s]ummary evidence need not be an exhibit, but may take the form of a witness's oral testimony.”). Third, the majority view is that the summaries themselves constitute the evidence of the contents of the materials summarized, rather than the underlying writings, recordings or photographs. *Id.* at § 1006.04[1] (“[t]he majority rule is that the summary itself is the evidence to be considered by the factfinder when the underlying documents are voluminous and the other requirements of Rule 1006 are met. Other decisions, however, have held that Rule 1006 summaries were not evidence, and that the jury should be so instructed.”). Fourth, if the summaries are accepted as the evidence of the materials summarized, they function as the equivalent of a special exception to the hearsay rule. *Id.* at § 1006.05[4] (“Rule 1006 should be regarded as a special exception to the hearsay rule.”); RICE at 197-98 (Recognizing that summaries of voluminous materials that are introduced to prove the content of the summarized material creates a hearsay problem. The author suggests that the residual hearsay rule, Rule 807, is an exception that may apply to overcome this problem). Fifth, the writings, recordings and photographs that are summarized must be made available to the adverse party for examination or copying reasonably in advance of the use of the summary, a requirement that originates from Rule 1006 itself, regardless of whether the adverse party has served a request for production of documents under FED.R.CIV.P. 34. WEINSTEIN at § 1006.06[1] (“the originals or duplicates of voluminous writings, recordings, or photographs must be made available for examination or copying at a reasonable time or place in order for summary evidence to be admissible. The right to examine the underlying records is absolute. Thus, the records must be made available whether or not the opposing party makes a discovery request for inspection.”). Sixth, the underlying materials from which the summaries are made must themselves be admissible into evidence. *Id.* at § 1006.06[3] (“Charts, summaries and calculations are only admissible when based on original or duplicate materials that are

themselves admissible evidence.”).

Because the production of electronically stored information in civil cases frequently is voluminous, the use of summaries under Rule 1006 is a particularly useful evidentiary tool, and courts can be expected to allow the use of summaries provided the procedural requirements of the rule are met. *See, e.g., Wapnick v. Comm'r of Internal Revenue, T.C. Memo. 2002-45, (T.C.2002)* (holding that summaries of voluminous computer records were admissible under Rule 1006 even though they were prepared in anticipation of litigation, because the underlying documents had been admitted into evidence and reasonably had been made available to the opposing party to inspect).

Rule 1007 identifies another, though little used, way in which secondary evidence may be used to prove the contents of electronically prepared or stored information. It provides that the:

“[c]ontents of writings, recordings, or photographs may be proved by the testimony or deposition of the party against whom offered or by that party's written admission,\*582 without accounting for the non-production of the original.”

On its face this rule is limited to admissions by a party opponent regarding the content of a writing, recording or photograph. Use of the word “admission” refers to any of the types of admissions covered by Rule 801(d)(2), which includes admissions by a representative, agent, employee or co-conspirator that meets the requirements of Rule 801(d)(2) for each of these types of admissions. WEINSTEIN at § § 1007.03[1], 1007.06. It does not require that any showing be made that the writing, recording or photograph is lost or otherwise unavailable. *Id.* at § 1007.04[1]. Further, the rule expressly limits the types of admissions that may be used to prove the contents of writings, recordings or photographs to those obtained during in court testimony, during a deposition,

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

or by the adverse party's written admission.<sup>FN57</sup> *Id.* at § 1007.04. An adverse party's answers to federal rule of civil procedure Rule 33 interrogatories or a Rule 36 request to admit the genuineness of documents would meet the provisions of Federal Rule of Evidence 1007 regarding a "written admission." *Id.* at § 1007.07 ("[A]n adverse party's responses to written interrogatories made pursuant to Federal Rule of Civil Procedure 33 are admissible to prove content. Similarly, an adverse party's responses to requests for admissions made pursuant to Federal Rule of Civil Procedure 36, are admissible to prove contents.").

FN57. However, despite the limitation in Rule 1007 to testimonial or written admissions of a party opponent, a non-testimonial oral admission by a party opponent would still be admissible as secondary evidence to prove the contents of a writing, recording or photograph under Rule 1004 if the writing, recording or photograph was lost or destroyed, absent bad faith, beyond the reach of court ordered production, in the possession, custody or control of the adverse party, or if the writing, recording or photograph was not closely related to a controlling issue in the litigation. FED.R.EVID. 1007 advisory committee's note ("The limitation [of] Rule 1007 to testimonial or written admissions, of course, does not call for excluding evidence of an oral admission when nonproduction of the original has been accounted for and secondary evidence generally has become admissible."); WEINSTEIN at § 1007.03[1].

Because Rule 1007 so seldom is used or discussed in cases, most lawyers are unaware of it. However, given the frequency with which deponents are asked questions about the content of writings, recordings and photographs, it is prudent to remember that if the deponent is a person whose testimony would qualify as an admission under any of the five varieties recognized by Rule 801(d)(2), then the deposition testimony

may be admitted to prove the contents of the writings, recordings and photographs described. The same is true for written responses to FED.R.CIV.P. 33 and 36 discovery that asks for a description of the contents of a writing, recording or photograph. The need is obvious, therefore, to insure that any characterization of the contents of a writing, recording or photograph that could fall within Rule 1007 be accurate.

Rule 1008 is the last of the rules in Article X of the rules of evidence. It states:

"When the admissibility of other evidence of contents of writings, recordings, or photographs under these rules depends upon the fulfillment of a condition of fact, the question whether the condition has been fulfilled is ordinarily for the court to determine in accordance with the provisions of rule 104. However, when an issue is raised (a) whether the asserted writing ever existed, or (b) whether another writing, recording, or photograph produced at the trial is the original, or (c) whether other evidence of contents correctly reflects the contents, the issue is for the trier of fact to determine as in the case of other issues of fact."

This rule is a specialized application of Rule 104(b), and it allocates responsibility between the trial judge and the jury with respect to certain preliminary matters affecting the original writing rule. As the advisory committee's note to Rule 1008 states:

"Most preliminary questions of fact in connection with applying the rule preferring the original as evidence of contents are for the judge, under the general principles announced in Rule 104[a]. Thus, the question whether the loss of the originals has been established, or of the fulfillment of other conditions specified in Rule 1004, \*583 *supra*, is for the judge. However, questions may arise which go beyond the mere administration of the rule preferring the original and into the merits of the controversy ... The latter portion of [Rule 1008] is designed to insure treatment of these situations as raising jury

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

questions. The decision is not one for uncontrolled discretion of the jury but is subject to the control exercised generally by the judge over jury determinations. *See* Rule 104(b)."

*See also* WEINSTEIN at § 1008.02[1]-1008.04[5]. Under the rule, the trial judge determines: whether originals have been lost or destroyed under Rule 1004(1), as well as all issues relating to the appropriateness of the proponent's efforts to search for the lost original;<sup>FN58</sup> whether or not the original is obtainable by judicial process, under Rule 1004(2);<sup>FN59</sup> whether the original is in the possession, custody or control of the opposing party under Rule 1004(3);<sup>FN60</sup> and whether the writing, recording or photograph relates to a collateral matter, which removes it from the reach of the original writing rule.<sup>FN61</sup>

FN58. WEINSTEIN at § 1008.04[3]

FN59. *Id.* at § 1008.04[4]

FN60. *Id.* at § 1008.04[5]

FN61. *Id.* at § 1008.04[6]

Rule 1008 identifies three issues that are questions for the jury, however: (1) whether the writing, recording or photograph ever existed in the first place; (2) whether some other writing, recording, or photograph that is offered into evidence is in fact the original; and (3) whether "other" (i.e. secondary) evidence of contents correctly reflects the content of the writing, recording or photograph. FED.R.EVID. 1008 advisory committee's note; WEINSTEIN at § 1008.05[1]. Counsel need to be aware of the different functions the judge and jury serve as they anticipate how to offer electronic writings, recordings and photographs into evidence. Given the challenges that often are associated with the authentication of electronically created or stored evidence, it is not unlikely

that there will be disputes of fact regarding whether an electronic writing ever existed in the first place, if the original cannot be produced and secondary evidence is offered, or when different versions of the same electronic document are offered into evidence by the opposing parties.

In summary, when counsel intend to offer electronic evidence at trial or in support of a motion for summary judgment they must determine whether the original writing rule is applicable, and if so, they must be prepared to introduce an original, a duplicate original, or be able to demonstrate that one of the permitted forms of secondary evidence is admissible. In this case, counsel did not address the original writing rule, despite its obvious applicability given that the e-mail exhibits were closely related to a controlling issue and there were proving the contents of the e-mails themselves.

The final evidentiary issue that must be considered in determining whether electronic evidence will be admitted is whether the probative value of the evidence is substantially outweighed by the danger of unfair prejudice, as proscribed under Rule 403 of the federal rules of evidence.

#### ***Balancing Probative Value Against the Danger of Unfair Prejudice Under Rule 403***

After evaluating the issues associated with relevance, authenticity, hearsay, and the original writing rule, the final step to consider with regard to electronically prepared or stored evidence is the need to balance its probative value against the potential for unfair prejudice, or other harm, under Rule 403 of the Federal Rules of Evidence. This rule states:

"Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446  
(Cite as: 241 F.R.D. 534)

cumulative evidence.”

FED.R.EVID. 403. The advisory committee note to Rule 403 succinctly explains its function:

“[C]ertain circumstances call for the exclusion of evidence which is of unquestioned relevance. These circumstances entail \*584 risks which range all the way from inducing decision on a purely emotional basis, at one extreme, to nothing more harmful than merely wasting time, at the other extreme. Situations in this area call for balancing the probative value of and need for the evidence against the harm likely to result from its admission.... ‘Unfair prejudice’ within its context means an undue tendency to suggest decision on an improper basis, commonly, though not necessarily an emotional one.”

See also WEINSTEIN at § 403.02[1][a].<sup>FN62</sup>

FN62. “Rule 403 recognizes that relevance alone does not ensure admissibility. A cost/benefit analysis must often be employed. Relevant evidence may be excluded if its probative value is not worth the problems that its admission may cause. The issue is whether the search for truth will be helped or hindered by the interjection of distracting, confusing, or emotionally charged evidence.”

A determination of whether evidence should be excluded under Rule 403 falls within the those made by the court under Rule 104(a), but it is used sparingly. WEINSTEIN at § 403.02[2][a]. Generally, “[i]f there is doubt about the existence of unfair prejudice, confusion of issues, misleading, undue delay, or waste of time, it is generally better practice to admit the evidence, taking necessary precautions of contemporaneous instructions to the jury followed by additional admonitions in the charge.” *Id.* at § 403.02[2][c].

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. *See Monotype Corp.*, 43 F.3d at 450 (Finding that trial court properly excluded an email from a Microsoft employee under Rule 403 that contained a “highly derogatory and offensive description of ... [another company's] type director.”); (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, *Friend v. Time Manufacturing Co.*, 2006 WL 2135807 at \*7 (D.Ariz.2006)(“Therefore, the question is simply whether the animation accurately demonstrates the scene of the accident, and whether the probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.”); *State v. Sayles*, 662 N.W.2d 1, 11 (Iowa, 2003) (Appellate court found no error in trial court's admission of computer animation slides showing effects of shaken infant syndrome, finding that trial court properly considered state version of Rule 403, and admitted evidence with a cautionary instruction that the evidence was only an illustration, not a re-creation of the actual crime); (3) when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 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 v. Johnny's Oyster and Shrimp Inc.*, 76 F.Supp.2d 773 (S.D.Tx.1999) (Court expressed extreme skepticism regarding the reliability and accuracy of information posted on the internet, referring to it variously as

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

(Cite as: 241 F.R.D. 534)

“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).

Thus, when a lawyer analyzes the admissibility of electronic evidence, he or she should consider whether it would unfairly prejudice the party against whom it is offered, confuse or mislead the jury, unduly delay the trial of the case, or interject collateral matters into the case. If a lawyer is offering electronic evidence, particularly computer animations, that may draw a Rule 403 objection, he or she must be prepared to demonstrate why any prejudice is not unfair, when measured against the probative value of the evidence. \*585 In this case, counsel did not address whether Rule 403 was implicated with respect to the electronic evidence attached to their summary judgment memoranda.

### *Conclusion*

[3] In this case the failure of counsel collectively to establish the authenticity of their exhibits, resolve potential hearsay issues, comply with the original writing rule, and demonstrate the absence of unfair prejudice rendered their exhibits inadmissible, resulting in the dismissal, without prejudice, of their cross motions for summary judgment. The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try. The Court hopes that the explanation provided in this memorandum order will assist in that endeavor.<sup>FN63</sup>

FN63. I acknowledge with gratitude the tireless assistance of two exceptionally talented law student interns, Ms. Puja Gupta and Mr. Ben Peoples, whose assistance in cite checking was invaluable, and my law clerk, Ms. Kathryn Widmayer, who consistently makes the most difficult tasks appear easy.

D.Md.,2007.

Lorraine v. Markel American Ins. Co.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

END OF DOCUMENT



Supreme Court of Connecticut.  
STATE of Connecticut  
v.  
Alfred SWINTON.

No. 16548.  
Argued Sept. 26, 2003.  
Decided May 11, 2004.

**Background:** Defendant was convicted following jury trial in the Superior Court, Judicial District of Hartford, Maloney, J., of murder.

**Holdings:** On direct appeal, the Supreme Court, Katz, J., held that:

- (1) enhanced photographs and computer generated overlays were demonstrative evidence rather than merely illustrative evidence and thus required proper foundation;
- (2) state laid an adequate foundation for enhancements of bite mark photograph;
- (3) testimony was insufficient to lay foundation to support admission of computer enhanced bite mark overlays;
- (4) error in admission of bite mark overlays did not violate defendant's confrontation rights but rather was merely evidentiary in nature;
- (5) error in admitting evidence of bite mark overlays without proper foundation was harmless error;
- (6) court did not improperly refuse to sequester victim's family member who was scheduled to testify as witness; and
- (7) jailhouse informant was not acting as police agent when he initially met with defendant, although he had been cooperating with police in connection with unrelated investigation.

Affirmed.

West Headnotes

[1] Criminal Law 110 388.1

110 Criminal Law  
110XVII Evidence  
110XVII(I) Competency in General  
110k388 Experiments and Tests; Scientific and Survey Evidence  
110k388.1 k. In general. Most Cited Cases

*Daubert* is only a threshold inquiry into the admissibility of scientific evidence and other evidentiary rules must also be satisfied.

[2] Criminal Law 110 339.6

110 Criminal Law  
110XVII Evidence  
110XVII(D) Facts in Issue and Relevance  
110k339.5 Identity of Accused  
110k339.6 k. In general. Most Cited Cases

Bite mark evidence, in general, is not unreliable or controversial.

[3] Criminal Law 110 338(1)

110 Criminal Law  
110XVII Evidence  
110XVII(D) Facts in Issue and Relevance  
110k338 Relevancy in General  
110k338(1) k. In general. Most Cited Cases

In determining the relevancy and admissibility of evidence, trial courts have broad discretion.

**[4] Criminal Law 110 ⚙️ 1153.1**

110 Criminal Law  
110XXIV Review  
110XXIV(N) Discretion of Lower Court  
110k1153 Reception and Admissibility of Evidence  
110k1153.1 k. In general. Most Cited Cases  
(Formerly 110k1153(1))

**Criminal Law 110 ⚙️ 1163(3)**

110 Criminal Law  
110XXIV Review  
110XXIV(Q) Harmless and Reversible Error  
110k1163 Presumption as to Effect of Error; Burden  
110k1163(3) k. Rulings as to evidence. Most Cited Cases

If the claim as to an evidentiary ruling is of constitutional magnitude, the state has the burden of proving the constitutional error was harmless beyond a reasonable doubt; otherwise, in order to establish reversible error on an evidentiary impropriety, the defendant must prove both an abuse of discretion and a harm that resulted from such abuse.

**[5] Criminal Law 110 ⚙️ 662.1**

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence  
110k662 Right of Accused to Confront Witnesses  
110k662.1 k. In general. Most Cited

Cases

The sixth amendment to the constitution of the United States guarantees the right of an accused in a criminal prosecution to be confronted with the witnesses against him; this right is secured for defendants in state criminal proceedings. U.S.C.A. Const.Amend. 6.

**[6] Criminal Law 110 ⚙️ 662.7**

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence  
110k662 Right of Accused to Confront Witnesses  
110k662.7 k. Cross-examination and impeachment. Most Cited Cases

The primary interest secured by confrontation is the right of cross-examination. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[7] Criminal Law 110 ⚙️ 444.16**

110 Criminal Law  
110XVII Evidence  
110XVII(P) Documentary Evidence  
110k444 Authentication and Foundation  
110k444.16 k. Photographs and videos. Most Cited Cases  
(Formerly 110k444)

The party moving to admit composite photographs as evidence must present witnesses with firsthand knowledge of how the composite was prepared and of how accurately it portrays that which it is intended to depict.

**[8] Criminal Law 110 ⚙️ 444.16**

110 Criminal Law  
110XVII Evidence  
110XVII(P) Documentary Evidence  
110k444 Authentication and Foundation  
110k444.16 k. Photographs and videos.  
Most Cited Cases  
(Formerly 110k444)

Under the foundational standard for photographs, all that is required is that a photograph be introduced through a witness competent to verify it as a fair and accurate representation of what it depicts.

**[9] Criminal Law 110 444.16**

110 Criminal Law  
110XVII Evidence  
110XVII(P) Documentary Evidence  
110k444 Authentication and Foundation  
110k444.16 k. Photographs and videos.  
Most Cited Cases  
(Formerly 110k444)

Enhanced photographs and computer generated overlays were demonstrative evidence rather than merely illustrative evidence and thus could not be admitted based on trial court opinion that they would assist the jury in understanding expert testimony, but rather required proper foundation.

**[10] Criminal Law 110 404.5**

110 Criminal Law  
110XVII Evidence  
110XVII(K) Demonstrative Evidence  
110k404.5 k. In general. Most Cited Cases

“Demonstrative evidence” is a pictorial or representational communication incorporated into a witness's testimony.

**[11] Criminal Law 110 404.5**

110 Criminal Law  
110XVII Evidence  
110XVII(K) Demonstrative Evidence  
110k404.5 k. In general. Most Cited Cases

Demonstrative evidence is not merely illustrative; it is just as much substantive evidence of the facts it depicts or portrays as is real or testimonial evidence.

**[12] Criminal Law 110 444.16**

110 Criminal Law  
110XVII Evidence  
110XVII(P) Documentary Evidence  
110k444 Authentication and Foundation  
110k444.16 k. Photographs and videos.  
Most Cited Cases  
(Formerly 110k444)

Court considered enhanced photographs as computer generated for purposes of foundation necessary for admission into evidence, as computer was both the process and the tool used to enable the enhanced photographs to be admitted.

**[13] Criminal Law 110 388.1**

110 Criminal Law  
110XVII Evidence  
110XVII(I) Competency in General  
110k388 Experiments and Tests; Scientific and Survey Evidence  
110k388.1 k. In general. Most Cited Cases

Federal standard for authentication or identification of a process or system can generally be satisfied by evidence that: (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 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. Fed.Rules Evid.Rule 901, 28 U.S.C.A.

**[14] Criminal Law 110 ⚙️388.1**

110 Criminal Law

110XVII Evidence

110XVII(I) Competency in General

110k388 Experiments and Tests; Scientific and Survey Evidence

110k388.1 k. In general. Most Cited Cases

Reliability is the watchword in determining the admissibility of computer generated evidence.

**[15] Criminal Law 110 ⚙️388.1**

110 Criminal Law

110XVII Evidence

110XVII(I) Competency in General

110k388 Experiments and Tests; Scientific and Survey Evidence

110k388.1 k. In general. Most Cited Cases

In order to lay a proper foundation for computer generated evidence, there must be testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer.

**[16] Criminal Law 110 ⚙️388.1**

110 Criminal Law

110XVII Evidence

110XVII(I) Competency in General

110k388 Experiments and Tests; Scientific and Survey Evidence

110k388.1 k. In general. Most Cited Cases

In addition to the reliability of computer generated evidence itself, what must be established is the reliability of the procedures involved, as defense counsel must have the opportunity to cross-examine the witness as to the methods used.

**[17] Criminal Law 110 ⚙️661**

110 Criminal Law

110XX Trial

110XX(C) Reception of Evidence

110k661 k. Necessity and scope of proof. Most Cited Cases

Trial courts must have considerable latitude in determining the admissibility of evidence.

**[18] Criminal Law 110 ⚙️444.16**

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.16 k. Photographs and videos. Most Cited Cases  
(Formerly 110k444)

State laid an adequate foundation for enhancements of bite mark photograph; expert testified that computer equipment was accepted as standard equipment in field and that program was relied upon by experts, it was established that qualified computer operator produced enhancement, there was evidence that proper procedures were followed in connection

with input and output of information, and state adequately demonstrated that program is a reliable software program.

**[19] Criminal Law 110 444.16**

110 Criminal Law  
110XVII Evidence  
110XVII(P) Documentary Evidence  
110k444 Authentication and Foundation  
110k444.16 k. Photographs and videos.  
Most Cited Cases  
(Formerly 110k444)

Expert testimony was insufficient to lay foundation to support admission of computer enhanced bite mark overlays at murder trial; expert could not testify as to whether computer processes used were accepted in the field of odontology, whether proper procedures were followed in connection with input and output of information, whether computer program was reliable for forensic application, whether the equipment was programmed and operated correctly, or whether qualified computer operator was employed, and program was capable of actually altering photographs.

**[20] Criminal Law 110 444.16**

110 Criminal Law  
110XVII Evidence  
110XVII(P) Documentary Evidence  
110k444 Authentication and Foundation  
110k444.16 k. Photographs and videos.  
Most Cited Cases  
(Formerly 110k444)

Expert's testimony that he was aware of computer imaging applications, was personally aware of their uses within the field of odontology, and that he had read papers in which the applications were used in bite mark analysis was inadequate to establish that the photo application had been proven reliable enough to

be deemed "competent" or that it had become standard practice in the field so that images created by application were admissible evidence.

**[21] Criminal Law 110 404.11**

110 Criminal Law  
110XVII Evidence  
110XVII(K) Demonstrative Evidence  
110k404.10 Foundation or Authentication  
110k404.11 k. In general. Most Cited Cases

**Witnesses 410 266**

410 Witnesses  
410III Examination  
410III(B) Cross-Examination  
410k266 k. Right to cross-examine and re-examine in general. Most Cited Cases

A witness must be able to testify, adequately and truthfully, as to exactly what the jury is looking at, and the defendant has a right to cross-examine the witness concerning the evidence.

**[22] Criminal Law 110 662.40**

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence  
110k662 Right of Accused to Confront Witnesses  
110k662.40 k. Use of documentary evidence. Most Cited Cases

Error in admission of bite mark overlays at murder trial did not violate defendant's confrontation rights but rather was merely evidentiary in nature, where overlays were just one part of expert's bite mark analysis, defendant had opportunity to cross-examine

expert as to bite marks, and defendant's own expert used overlays to support conclusion that bite marks were not left by defendant. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[23] Criminal Law 110 ⚔ 662.1**

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence  
110k662 Right of Accused to Confront  
Witnesses  
110k662.1 k. In general. Most Cited  
Cases

The right to confrontation is fundamental to a fair trial under both the federal and state constitutions. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[24] Constitutional Law 92 ⚔ 3856**

92 Constitutional Law  
92XXVII Due Process  
92XXVII(A) In General  
92k3848 Relationship to Other Constitu-  
tional Provisions; Incorporation  
92k3856 k. Sixth Amendment. Most  
Cited Cases  
(Formerly 92k268(10))

The confrontation clause of the sixth amendment is made applicable to the states through the due process clause of the fourteenth amendment. U.S.C.A. Const.Amend. 6, 14.

**[25] Criminal Law 110 ⚔ 662.7**

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence

110k662 Right of Accused to Confront  
Witnesses

110k662.7 k. Cross-examination and  
impeachment. Most Cited Cases

The defendant is entitled fairly and fully to confront and to cross-examine the witnesses against him. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[26] Criminal Law 110 ⚔ 662.7**

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence  
110k662 Right of Accused to Confront  
Witnesses  
110k662.7 k. Cross-examination and  
impeachment. Most Cited Cases

The confrontation clause requires that the defendant be accorded some irreducible minimum of cross-examination into matters affecting the reliability and credibility of the state's witnesses. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[27] Witnesses 410 ⚔ 266**

410 Witnesses  
410III Examination  
410III(B) Cross-Examination  
410k266 k. Right to cross-examine and  
re-examine in general. Most Cited Cases

The defendant's right to cross-examine a witness is not absolute. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[28] Criminal Law 110 ⚔ 662.7**

110 Criminal Law

110XX Trial

110XX(C) Reception of Evidence

110k662 Right of Accused to Confront  
Witnesses

110k662.7 k. Cross-examination and  
impeachment. Most Cited Cases

In order to comport with the constitutional standards embodied in the confrontation clause, the trial court must allow a defendant to expose to the jury facts from which the jurors, as the sole triers of fact and credibility, could appropriately draw inferences relating to the reliability of the witness. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

[29] Witnesses 410 ⚡ 266

410 Witnesses

410III Examination

410III(B) Cross-Examination

410k266 k. Right to cross-examine and  
re-examine in general. Most Cited Cases

In determining whether a defendant's right of cross-examination has been unduly restricted, the court considers the nature of the excluded inquiry, whether the field of inquiry was adequately covered by other questions that were allowed, and the overall quality of the cross-examination viewed in relation to the issues actually litigated at trial. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

[30] Criminal Law 110 ⚡ 662.7

110 Criminal Law

110XX Trial

110XX(C) Reception of Evidence

110k662 Right of Accused to Confront  
Witnesses

110k662.7 k. Cross-examination and  
impeachment. Most Cited Cases

Foundational questions are generally of an evidentiary nature, and, in most instances, a mere evidentiary error will not rise to the level of a constitutional error.

[31] Criminal Law 110 ⚡ 1169.1(10)

110 Criminal Law

110XXIV Review

110XXIV(Q) Harmless and Reversible Error

110k1169 Admission of Evidence

110k1169.1 In General

110k1169.1(10) k. Documentary and  
demonstrative evidence. Most Cited Cases

Evidentiary error in admitting evidence of bite mark overlays without proper foundation was harmless error at murder trial, where bite mark expert properly and extensively testified as to bite mark evidence other than overlays and testified "without any reservation" that bite marks were created by defendant's teeth, physical evidence including bra, trash bags, and safety pins linked defendant to victim, defendant had made numerous incriminating statements and confessions, and defendant revealed his anger toward woman and prostitutes to many witnesses.

[32] Criminal Law 110 ⚡ 1168(1)

110 Criminal Law

110XXIV Review

110XXIV(Q) Harmless and Reversible Error

110k1168 Rulings as to Evidence in General

110k1168(1) k. In general. Most Cited  
Cases

In order to establish reversible error on an evidentiary impropriety, the defendant must demonstrate that it is more probable than not that the erroneous action of the court affected the result.

[33] Criminal Law 110 ⚡ 1170.5(1)

110 Criminal Law  
110XXIV Review  
110XXIV(Q) Harmless and Reversible Error  
110k1170.5 Witnesses  
110k1170.5(1) k. In general. Most Cited Cases

Defendant was not harmed by trial court's failure to mark as an exhibit police reports which were not offered into evidence but which were used by lead investigator to refresh his recollection on direct examination, despite defendant's claim that failure to mark items deprived him of opportunity to preserve for appellate review which documents investigator used, as investigator stated that documents were police reports he personally had authored, and all reports previously had been disclosed to defendant.

[34] Criminal Law 110 ⚔ 627.8(4)

110 Criminal Law  
110XX Trial  
110XX(A) Preliminary Proceedings  
110k627.5 Discovery Prior to and Incident to Trial  
110k627.8 Proceedings to Obtain Disclosure  
110k627.8(4) k. Examination by court; inspection in camera. Most Cited Cases

Trial court did not abuse discretion in refusing to turn over to defense limited portions of witness's two letters written to an inspector in the state's attorney's office which were related to the ongoing investigation of other crimes, as excised material did not relate to subject matter of witness's testimony and redaction of letters was necessary to maintain secrecy regarding informants as required for effective investigation of criminal activity. Practice Book 1998, § 40-41(3).

[35] Criminal Law 110 ⚔ 665(1)

110 Criminal Law  
110XX Trial  
110XX(C) Reception of Evidence  
110k665 Separation and Exclusion of Witnesses  
110k665(1) k. Power and duty of court. Most Cited Cases

Trial court did not improperly refuse to sequester victim's family member who was scheduled to testify as witness at murder trial, although defendant twice sought a sequestration of "any and all potential witnesses," as court expressly indicated a willingness to consider any additional motions for sequestration and encouraged state and defendant to be vigilant about making such requests, but defendant failed to request specifically that particular witness be sequestered. C.G.S.A. Const. Art. 1, § 8; C.G.S.A. §§ 54-85a, 54-85f.

[36] Criminal Law 110 ⚔ 1710

110 Criminal Law  
110XXXI Counsel  
110XXXI(B) Right of Defendant to Counsel  
110XXXI(B)1 In General  
110k1710 k. In general. Most Cited Cases  
(Formerly 110k641.7(1))

Once the right to counsel has attached, the Sixth Amendment imposes on the state an affirmative obligation to respect and preserve the accused's choice to seek the assistance of counsel. U.S.C.A. Const.Amend. 6.

[37] Criminal Law 110 ⚔ 411.86(6)

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and

Admissions by or on Behalf of Accused  
110XVII(M)16 Invocation of Rights  
110k411.82 Effect of Invocation  
110k411.86 Reinitiating Interrogation  
110k411.86(6) k. Initiation by  
defendant. Most Cited Cases  
(Formerly 110k412.2(4))

A violation of the right to counsel can arise even if it is the accused who initiates the conversation with the undisclosed state agent after the right to counsel has attached. U.S.C.A. Const.Amend. 6.

**[38] Criminal Law 110 411.31**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and  
Admissions by or on Behalf of Accused  
110XVII(M)12 Counsel in General  
110k411.31 k. Absence or denial of  
counsel. Most Cited Cases  
(Formerly 110k412.2(4))

The knowing exploitation by the state of an opportunity to confront the accused without counsel being present is as much a breach of the state's obligation not to circumvent the right to the assistance of counsel as is the intentional creation of such an opportunity. U.S.C.A. Const.Amend. 6.

**[39] Criminal Law 110 1158.1**

110 Criminal Law  
110XXIV Review  
110XXIV(O) Questions of Fact and Findings  
110k1158.1 k. In general. Most Cited Cases  
(Formerly 110k1158(1))

When a defendant raises a question on appeal that is vitally affected by trial court factfinding, in a setting in which the credibility of the witnesses is not the

primary issue, the Supreme Court's customary deference to the trial court is tempered by the necessity for a scrupulous examination of the record to ascertain whether such a factual finding is supported by substantial evidence.

**[40] Criminal Law 110 411.67**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and  
Admissions by or on Behalf of Accused  
110XVII(M)15 Persons to Whom Made  
110k411.67 k. Informants; inmates.  
Most Cited Cases  
(Formerly 110k412.2(4))

The existence of an agency relationship between the police and an informant, so that the informant's questioning of a defendant violates the right to counsel, turns upon a number of factual inquiries into the extent of police involvement with the informant, including the following: whether the police have promised the informant a reward for his cooperation or whether he is self-motivated, whether the police have asked the informant to obtain incriminating evidence and placed him in a position to receive it, and whether the information is secured as part of a government initiated, pre-existing plan. U.S.C.A. Const.Amend. 6.

**[41] Criminal Law 110 411.67**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and  
Admissions by or on Behalf of Accused  
110XVII(M)15 Persons to Whom Made  
110k411.67 k. Informants; inmates.  
Most Cited Cases  
(Formerly 110k412.2(4))

There is no bright line test by which the deter-

mination of whether a police informant deliberately elicited a defendant's statements absent the presence of counsel is made; rather, the court scrutinizes the record to determine whether the exchanges between the defendant and the informant look like government interrogations. U.S.C.A. Const.Amend. 6.

**[42] Criminal Law 110 411.67**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and Admissions by or on Behalf of Accused  
110XVII(M)15 Persons to Whom Made  
110k411.67 k. Informants; inmates.  
Most Cited Cases  
(Formerly 110k412.2(4))

Jailhouse informant was not acting as police agent when he initially met with murder defendant, although he had been cooperating with police in connection with unrelated investigation, and thus conversation with defendant did not violate defendant's right to counsel, where government had not directed or steered informant towards defendant, but rather informant had hoped to gather information to give to government in exchange for an expected benefit. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[43] Criminal Law 110 411.67**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and Admissions by or on Behalf of Accused  
110XVII(M)15 Persons to Whom Made  
110k411.67 k. Informants; inmates.  
Most Cited Cases  
(Formerly 110k412.2(4))

Jailhouse informant had not elicited defendant incriminating statements after becoming government

agent, and thus statements were not made in violation of defendant's right to counsel; informant was no more than passive listener to defendant. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[44] Criminal Law 110 411.67**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and Admissions by or on Behalf of Accused  
110XVII(M)15 Persons to Whom Made  
110k411.67 k. Informants; inmates.  
Most Cited Cases  
(Formerly 110k412.2(4))

A defendant does not make out a constitutional violation of his right to counsel simply by showing that an informant, either through prior arrangement or voluntarily, reported the defendant's incriminating statements to the police.

**[45] Criminal Law 110 411.67**

110 Criminal Law  
110XVII Evidence  
110XVII(M) Statements, Confessions, and Admissions by or on Behalf of Accused  
110XVII(M)15 Persons to Whom Made  
110k411.67 k. Informants; inmates.  
Most Cited Cases  
(Formerly 110k412.2(4))

**Criminal Law 110 1721**

110 Criminal Law  
110XXXI Counsel  
110XXXI(B) Right of Defendant to Counsel  
110XXXI(B)2 Stage of Proceedings as Affecting Right  
110k1721 k. Investigative proceedings generally; witness interviews; search or surveillance;

cavesdropping and use of informers. Most Cited Cases  
(Formerly 110k641.3(7))

Although the government has an affirmative obligation not to solicit incriminating statements from the defendant in the absence of his counsel, there is no constitutional violation when a government informant merely listens and reports. U.S.C.A. Const.Amend. 6; C.G.S.A. Const. Art. 1, § 8.

**[46] Criminal Law 110 1171.1(1)**

110 Criminal Law  
110XXIV Review  
110XXIV(Q) Harmless and Reversible Error  
110k1171 Arguments and Conduct of Counsel  
110k1171.1 In General  
110k1171.1(1) k. Conduct of counsel in general. Most Cited Cases

To prove prosecutorial misconduct, the defendant must demonstrate substantial prejudice; in order to demonstrate this, the defendant must establish that the trial as a whole was fundamentally unfair and that the misconduct so infected the trial with unfairness as to make the conviction a denial of due process. U.S.C.A. Const.Amend. 14.

**[47] Criminal Law 110 1171.1(1)**

110 Criminal Law  
110XXIV Review  
110XXIV(Q) Harmless and Reversible Error  
110k1171 Arguments and Conduct of Counsel  
110k1171.1 In General  
110k1171.1(1) k. Conduct of counsel in general. Most Cited Cases

Prosecutorial misconduct of constitutional proportions may arise during the course of closing ar-

gument, thereby implicating the fundamental fairness of the trial itself. U.S.C.A. Const.Amend. 14.

**[48] Criminal Law 110 2089**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel  
110k2088 Matters Not Sustained by Evidence  
110k2089 k. In general. Most Cited Cases  
(Formerly 110k719(1))

While the privilege of counsel in addressing the jury should not be too closely narrowed or unduly hampered, it must never be used as a license to state, or to comment upon, or to suggest an inference from, facts not in evidence, or to present matters which the jury have no right to consider.

**[49] Criminal Law 110 2117**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel  
110k2102 Inferences from and Effect of Evidence  
110k2117 k. Homicide and assault with intent to kill. Most Cited Cases  
(Formerly 110k720(9))

Prosecution's assertion that murder trial was "a case about a vicious murder of a young woman, the mother of two young children, who was lured into a sinister trap, beaten, stripped, sexually assaulted and violently strangled until the breath of life was gone" was not prosecutorial misconduct, as that was precisely what the case involved.

**[50] Criminal Law 110 ⚔ 2153**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel  
110k2145 Appeals to Sympathy or Prejudice  
110k2153 k. Attacks on opposing counsel. Most Cited Cases  
(Formerly 110k723(1))

Prosecutor's remark that "we've seen tactics in this courtroom that have gone from plants in the courtroom to demonstrations by counsel where the results are hidden" was supported by record and did not constitute prosecutorial misconduct, as series of events had occurred that included defendant's failed attempt to impeach witness regarding a conversation he had during a recess and an equally unsuccessful bite that defense counsel inflicted upon his own arm, the result of which he thereafter refused to show to the jury upon the state's request.

**[51] Criminal Law 110 ⚔ 2091**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel  
110k2088 Matters Not Sustained by Evidence  
110k2091 k. Personal knowledge, opinion, or belief of counsel. Most Cited Cases  
(Formerly 110k719(3))

**Criminal Law 110 ⚔ 2098(5)**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel

110k2093 Comments on Evidence or Witnesses

110k2098 Credibility and Character of Witnesses; Bolstering

110k2098(5) k. Credibility of other witnesses. Most Cited Cases  
(Formerly 110k720(5))

Prosecutor's assertion at murder trial that "there's no way that the truth is going to be hidden, not by me in a criminal trial" was not improper attempt by prosecutor to vouch for the strength of the state's case and witnesses; rather, remark was in connection with the state's discussion of the victim's lifestyle, which the state did not attempt to hide.

**[52] Criminal Law 110 ⚔ 2117**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel  
110k2102 Inferences from and Effect of Evidence  
110k2117 k. Homicide and assault with intent to kill. Most Cited Cases  
(Formerly 110k720(9))

**Criminal Law 110 ⚔ 2143**

110 Criminal Law  
110XXXI Counsel  
110XXXI(F) Arguments and Statements by Counsel  
110k2140 Comments on Character or Conduct

110k2143 k. Character, conduct, or appearance of accused. Most Cited Cases  
(Formerly 110k722.3)

**Criminal Law 110 ⚔ 2149**

110 Criminal Law

110XXXI Counsel

110XXXI(F) Arguments and Statements by  
Counsel

110k2145 Appeals to Sympathy or Preju-  
dice

110k2149 k. Comments on character of  
offense charged. Most Cited Cases  
(Formerly 110k723(2))

State did not improperly suggest that murder defendant still clung to a conspiracy theory despite his attorney's express rejection of such a defense, or improperly inject passion by referring to murder victim's bra as the defendant's trophy, as they were a fair summary of the defendant's case and his conduct.

**\*\*926** James B. Streeto, assistant public defender, for the appellant (defendant).

Christopher T. Godialis, assistant state's attorney, with whom were John M. Massameno, senior assistant state's attorney, and, on the brief, Christopher L. Morano, chief state's attorney, John M. Bailey, former chief state's attorney, and Carolyn K. Longstreth, former senior assistant state's attorney, for the appellee (state).

SULLIVAN, C.J., and BORDEN, KATZ, PALMER  
and VERTEFEUILLE, Js.

**\*\*927** KATZ, J.

**\*784** The defendant, Alfred Swinton, appeals <sup>FN1</sup> from the judgment of conviction, rendered after a jury trial, of one count of murder in violation of General Statutes § 53a–54a. <sup>FN2</sup> The defendant claims on appeal that the trial court improperly: (1) admitted into evidence computer enhanced photographs and computer generated exhibits without a proper foundation; (2) refused to mark a file as a court exhibit for appellate review; **\*785** 3) failed fully to disclose all relevant material for cross-examination following its in camera

review of a witness' out-of-court statements; (4) failed to sequester members of the victim's family who were scheduled to testify as witnesses at trial; and (5) failed to grant the defendant's motion to suppress certain statements that he had made to a fellow inmate while the defendant was incarcerated during trial. In addition, the defendant claims that the state's attorney committed prosecutorial misconduct in his argument to the jury. We reject the defendant's claims and, accordingly, we affirm the judgment of the trial court.

FN1. The defendant appealed directly to this court pursuant to General Statutes § 51–199(b), which provides in relevant part: “The following matters shall be taken directly to the Supreme Court ... (3) an appeal in any criminal action involving a conviction for a capital felony, class A felony, or other felony, including any persistent offender status, for which the maximum sentence which may be imposed exceeds twenty years....”

FN2. General Statutes § 53a–54a (a) provides in relevant part: “A person is guilty of murder when, with intent to cause the death of another person, he causes the death of such person....”

The jury reasonably could have found the following facts. On January 12, 1991, the twenty-eight year old victim, Carla Terry, left her residence for an evening out. She was dressed in a black brassiere, white underwear, a blue shirt, jeans, socks, boots, a white hat, and multiple jackets. The victim's sister, Laverne Terry, had helped the victim adjust the size of the black bra by inserting two safety pins into the right side of the garment. Later that night, the victim encountered Hector Freeman, her neighbor, at the Oakland Terrace Café in Hartford. The two proceeded to the Keney Park Cafe, arriving there after 1 a.m. on January 13, 1991. Once inside, Freeman and the victim separated. At some point during the evening, the

defendant was seen speaking with the victim. At approximately 2 a.m., Freeman and the victim left the bar together. The defendant left moments thereafter. Freeman gave the victim a ride home. The victim's sister, Rhonda Terry, heard the victim arrive outside of her apartment "[a] little after two" in the morning and, through a window, watched the victim get out of Freeman's car. The victim called out to her sister that she would return shortly and that she was going to stay with her sister that night. She then walked across the street and out of view.

\*786 At approximately 4:45 a.m. on January 13, 1991, Officer Michael Matthews of the Hartford police department found the victim's body in a snow bank near the University of Hartford—an area identified as being near one of the defendant's previous addresses. The victim was partially dressed, her undergarments had been removed, and she was wrapped in a brown plastic garbage bag. Paramedics arrived, and after an unsuccessful attempt to revive her, they took the victim to the hospital, where she was pronounced dead.

Edward McDonough, deputy chief medical examiner for the state, conducted an autopsy and concluded that the cause of death was asphyxia by manual strangulation. Taking into account the twenty-seven degree temperature of that evening and early morning, he estimated the time of \*\*928 death as approximately two or three hours before the victim's body arrived at the hospital. McDonough noted bruising on the victim's scalp consistent with blows to the head, as well as abrasions on the victim's neck, and bruising on her face and elsewhere on her body. In particular, McDonough observed and photographed crescent shaped bruises on each of the victim's breasts that he identified as being consistent with bite marks. The bite marks had been inflicted at or near the time of death. McDonough consulted with Lester Luntz, a forensic odontologist,<sup>FN3</sup> regarding the bruises on the victim's breasts. Ultimately, Luntz identified the bruises as bite marks.

FN3. Forensic odontology is the application of the law to the field of dentistry. It includes the analysis of dentition and bite marks for purposes of identification.

On January 19, 1991, following an initial investigation that revealed that the defendant had been in the Keney Park Cafe the night of the victim's murder, Detectives James Rovella and Stephen Kumnick of the Hartford police department interviewed the defendant at his residence\*787 in Stafford Springs. The police conducted a second interview approximately one week later at the police station. During interviews with the police, the defendant repeatedly mentioned an altercation that he had had with his former wife and that, even though the police report memorializing the incident stated that he had "choked" her, the defendant claimed that he actually had restrained her instead. Following the second interview, the police sought and obtained several search warrants for the defendant's residence. On March 5, 1991, the police executed a warrant for the defendant's residence, and the common areas of the building were searched with the consent of the building owner. During the course of the search of the common basement area to which the defendant had access, the police found a cardboard box containing a black bra that had holes in the cloth that could have been made by safety pins. Laverne Terry, the victim's sister, who had helped the victim adjust her bra before she went out for the evening, identified it as the same bra the victim had worn on the night of her murder. The police also found brown plastic garbage bags located in a shed behind the defendant's residence, and safety pins in the defendant's van. In addition, the police found a newspaper in the defendant's apartment dated the day of the victim's death, but found no other editions of the newspaper.

Also pursuant to a warrant, Luntz made molds,<sup>FN4</sup> or models, of the defendant's teeth. Following Luntz' death, the molds of the defendant's teeth were retrieved from Luntz' house by the police. These molds

were examined later by another forensic odontologist, Constantine Karazulas, who concluded that the defendant had inflicted the bite marks on the victim's body.

FN4. To create these molds, Luntz first took impressions of the defendant's teeth in a silicone material. A form of plaster known as "dental stone" then was poured into the impression and left to harden into molds.

\*788 Over the next several years,<sup>FN5</sup> the defendant made several incriminating statements. While being transported to get molds of his teeth made, the defendant made comments to Lieutenant Jose Lopez of the Hartford police department that women "bore the seed of ... evil." The \*\*929 defendant stated that women were always looking for favors and that sex was the only thing women had to offer in exchange for such favors. The defendant told Lopez that someone like the victim had used him for money and for rides, and that women like that "get what they deserve." The defendant labeled these women prostitutes and included the victim in this class. He seemed angry that women had used him in this manner. In June, 1992, the defendant arrived at Benton Auto Body, a towing company and auto body shop that worked in conjunction with the Hartford police department, in order to pick up his van that was to be released to him after a "police hold." The defendant told Ann Fraczek, the manager of the towing company, that he had been accused of biting a woman on the breast and then murdering her. He admitted that he had dated the victim and that she had been in his van. The defendant also stated that the police had "fouled the whole investigation up" and had done a "lousy job." As he was leaving, he told Fraczek that the police had "screwed up so bad they will never catch me now...."

FN5. Although the defendant originally was charged with murder in June, 1991, that charge was dismissed following a finding of no probable cause. It was not until October,

1998, that the defendant was rearrested for the homicide.

The defendant also made certain incriminating statements during a 1993 interview with Karon Haller, a freelance writer working with Connecticut Magazine.<sup>FN6</sup> The interview took place over dinner and several drinks, \*789 and the defendant spoke with Haller concerning the victim's murder, hoping to enlist her help in proving that he was innocent of that crime. During the discussion, the defendant ruminated vaguely over who might have committed the crime, and why. His rumination was interspersed with frequent, and often incoherent, digressions concerning prostitution, sex and drug use, and its peculiar effect on a person's sense of reality. The defendant suggested that the victim was a drug user and a prostitute, and that she might have taken money from the killer and then not fulfilled her promise of sex. He theorized that she probably had offered sex in exchange for money, but then had tried to "skip out" with the money. The defendant's most incriminating remarks came at a particular point in the interview at which he pleaded with Haller for help in his investigation into who murdered the victim, and he offered her all the information that he previously had gathered on the subject. In response, Haller asked whether the killer was going to "do it again." The defendant responded: "Summer's long, and summer's hot." Haller asked: "Why? Why doesn't he just stop?" The defendant answered: "If I knew that, I can stop tomorrow. If I knew that, I would stop tomorrow.... So somebody could live."

FN6. Haller's interview was introduced as evidence in redacted form because the defendant was a suspect in other uncharged murders, and the interview referred both to the charged murder and uncharged crimes as well.

In addition, on more than one occasion, the defendant declared to various acquaintances that he had

“gotten away” with murder. For example, Mary Alice Mills, an admitted drug addict who stole and engaged in prostitution to support her addiction, stated that, in the summer of 1991, while drinking and doing drugs with a group of people, the defendant said he had “got away with killing” the victim, and that he had killed her because “[h]e didn't like women anymore.”<sup>FN7</sup> In addition, Cynthia Stallings, also a drug user, stated that the defendant \*790 had made derogatory remarks about women in her presence. Shortly after the initial murder charge against the defendant was dismissed; see footnote 5 of this opinion; Stallings and a \*\*930 group of people, including the defendant, sat in her mother's bedroom drinking. Someone in the group had mentioned the victim's name, and the defendant started laughing. Somebody told the defendant that he should not laugh, even if he was innocent of the charge, because the victim was dead. The defendant replied, smirking, that he was not innocent, and that the police “had [him] for the teeth marks on her [breast],” but that the authorities had made mistakes.

FN7. Mills said that the defendant had been one of her “customers.” She also admitted to having “taken advantage” of him on several occasions.

On another occasion, Stallings and a friend, Sonia Faye Henderson, were out at a bar when they saw the defendant. Despite Stallings' warnings to Henderson that the defendant had been charged with murder, Henderson sat drinking and smoking with the defendant. When the bar closed, Henderson left and got into the defendant's car with him. Stallings rode in a car that traveled immediately in front of the defendant's car. At some point, Stallings noticed the defendant's car weaving, and saw that the defendant and Henderson were struggling with each other inside the defendant's car. Stallings got out of the car she was in and approached the defendant's car. When she opened the passenger car door, she saw that the defendant had his hands on Henderson's neck and Henderson was struggling to get out of the car. Henderson was yelling

for the defendant to let her go, and the defendant was yelling that he had spent money on her and expected a sexual favor in return. Henderson appeared to be hysterical, as she was hollering and crying. Stallings grabbed Henderson and yanked her from the defendant's grip, eventually pulling her out of the car. The defendant laughed and drove away. After the incident, Henderson's neck looked red, scratched and swollen.

\*791 The defendant's coworkers also recounted incriminating behavior by the defendant. Andrew Brescia met the defendant while working as a remodeler and general contractor at a property in Stafford Springs. After he became aware that the defendant was a suspect in a murder investigation, he would make teasing remarks toward the defendant, including calling him “choking Al.” On one particular occasion, he asked the defendant what it was like to strangle a woman. In response, the defendant said, “ ‘You want to know what it feels like? I'll show you,’ ” and grabbed Brescia from behind and started to choke him. The defendant applied a lot of pressure to Brescia's neck, in what Brescia described as a “grip of steel.” According to Brescia, the defendant did not appear to be joking. Edward Manner, the defendant's landlord, who employed both the defendant and Brescia, witnessed this incident. Manner also stated that once, over lunch, he had asked the defendant what it was like to rape and kill a woman, and that the defendant merely grinned and laughed in response.

In February, 1991, the defendant made incriminating statements to his brother, Larry Swinton, while they were in the presence of James Arnold, an acquaintance of the defendant and an admitted heroin addict. According to Arnold, Larry Swinton called the defendant stupid for beating up and biting the victim, and the defendant responded that, although he had done these things to the victim, she was alive when he left her. Arnold recounted other conversations relating to the victim, in which the defendant had explained that she had made him angry by calling him stupid and other names, and that he was tired of women playing

games with him. According to Arnold, the defendant was very angry at women who would take his money or who would allow him to buy them drinks or drugs, and then not follow through on their promises of sex. The defendant also told Arnold that he had “just lost it” and \*792 regretted what he had \*\*931 done, but that he had not killed the victim. During another conversation with Arnold, the defendant discussed having had rough sex with the victim and stated that the victim had gotten angry with him over something pertaining to the sex act.<sup>FN8</sup>

FN8. Arnold also told police that between 1989 and 1992, the defendant would often carry with him a brown valise that he closely guarded. He carried the valise everywhere he went, including into the bathroom. One evening, when the defendant fell asleep, Arnold and another individual opened the valise and viewed its contents. The valise was filled with women's undergarments and lingerie of various styles and colors, as well as magazines containing explicit and violent sexual material.

Following his arrest in 1998; see footnote 5 of this opinion; the defendant also made several incriminating statements to a fellow inmate, Michael Scalise, while the defendant was imprisoned during his trial.<sup>FN9</sup> In particular, on January 31, 2001, after his trial had begun, the defendant told Scalise that he was going to have his son kill two witnesses who had testified against him, including one of the victim's sisters. Scalise reported this information to a correction officer on or about February 7, 2001. On February 13, 2001, Scalise reported that he had more information beyond the threats the defendant had made. As a consequence, on February 16, 2001, Scalise met with Detective Rovella and Eric Daigle, a state police trooper, to divulge a number of incriminating statements made by the defendant about which Scalise later testified. Specifically, the defendant confessed to Scalise that he had killed the victim, wrapped her in a

plastic bag, and left her in a snow bank near a college. The defendant also revealed to Scalise that he had bitten the victim during sexual intercourse prior to killing her. The defendant demonstrated to Scalise how he had strangled the victim with his \*793 hands. He bragged to Scalise that he “got her good.” The defendant revealed that he had redressed the victim, and had put her jackets back on, to keep her warm. He also admitted to keeping the victim's bra and panties for “mementos.”

FN9. Although Scalise acknowledged that some of his trial testimony was more detailed than the written statements that memorialized his conversations with the police, Scalise testified that he had not learned of any details of the crime from the media's reporting of the defendant's trial and that his only source of information concerning the homicide was the defendant.

The defendant also stated to Scalise that the state would not be able to prove its case after ten years had passed. He believed that the state would not be able to match his teeth to the bite marks on the victim's body, and he showed Scalise prints of his teeth and a letter from a forensic analyst in support of his contention. The defendant told Scalise that he was having some of his teeth pulled, so that if the state took more molds of his teeth, the new molds would not match up with the bite marks on the victim. The defendant also kept his head shaved while in jail because he believed it would prevent the police from obtaining any further hair samples from him. The defendant revealed to Scalise that the police had found the same type of plastic bag at his house, but that he thought he had a solid defense because the bag was a common household item. The defendant admitted to meeting the victim at a bar, and stated that, even though he had committed the crime, the police should not have singled him out because there were many other people at the bar the night she was killed. He further stated his belief that the victim's sister could not remember the bra the victim had worn

ten years earlier.

Scalise met with Rovella and Daigle again on February 22, 2001, at which point \*\*932 he disclosed additional incriminating information about the defendant and memorialized his disclosures in written statements. The defendant had explained to Scalise that, on the night of the victim's murder, he had gone to the bar alone, and the victim had arrived with another man. The victim had left the bar that night with the other man, but the defendant had met up with the victim later that night, \*794 whereupon he had sex with her, killed her, "bagged" her, and then "dumped" her body in a snow bank near the University of Hartford. The defendant also revealed that he had been angry and jealous because the man the victim had been seen with earlier was married, and the defendant had believed that the man had "no business spending time" with the victim. The defendant told Scalise that he had bitten the victim on her breast while having sex with her, had beaten her in the face, and had strangled her. He also admitted to having had sex with the victim on previous occasions in exchange for drugs. The defendant stated that, after he had killed the victim, he took her bra and underwear, and that a safety pin had been attached to the bra. He told Scalise that he had taken the pin off the bra and used it in his van to pierce his radiator.

The defendant was convicted of murder and sentenced to a term of sixty years imprisonment. This appeal followed. Additional facts will be set forth as necessary.

## I

The defendant first claims that the trial court improperly admitted into evidence computer enhanced photographs <sup>FN10</sup> and computer generated exhibits without an adequate foundation. Specifically, the defendant challenges the admissibility of two separate, but related, pieces of evidence: first, photographs of a bite mark <sup>FN11</sup> on the victim's body that were enhanced using a computer software program known

as Lucis, and second, images \*795 of the defendant's teeth overlaid, or superimposed, upon photographs of the bite mark that were made through the use of Adobe Photoshop, another computer software program. The defendant contends that the state did not present foundation testimony on the adequacy of these two programs for the task of matching the defendant's dentition with the victim's bite mark because the computer enhanced and computer generated exhibits were introduced through experts with no more than an elementary familiarity with the programs. Therefore, the defendant argues, the admission of this evidence violated his constitutional right to confrontation. The state responds that the exhibits were merely photographic or illustrative evidence, not scientific evidence, and therefore did not require the testimony of a witness who could explain the inner workings of the equipment that produced it in order to provide an adequate foundation. We conclude that the trial court properly admitted into evidence the computer enhanced photographs, but improperly admitted the superimposed images created by Adobe Photoshop.

FN10. The state contends that the defendant's objection concerning the Lucis enhanced photographs was unpreserved. On the basis of our review of the record, including the trial court's express ruling on the defendant's objection to the photographs, we conclude that this claim was raised at trial and therefore properly was preserved for appellate review.

FN11. The photograph of the victim's left breast actually revealed two separate bite marks; for identification and comparative purposes, however, only the bite mark closest to the nipple was used. See footnote 34 of this opinion.

[1][2] According to the defendant, the law governing the admissibility of scientific evidence is applicable to the question of \*\*933 admissibility of computer enhanced and computer generated evidence.

The dominant standard for determining the admissibility of scientific evidence is *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993). In *Daubert*, the United States Supreme Court concluded that a two part inquiry should govern the admissibility of scientific evidence: “whether the reasoning or methodology underlying the testimony is scientifically valid and ... whether that reasoning or methodology properly can be applied to the facts in issue.” *Id.*, at 592–93, 113 S.Ct. 2786. We adopted this standard in *State v. Porter*, 241 Conn. 57, 68, 698 A.2d 739 (1997), cert. denied, \*796523 U.S. 1058, 118 S.Ct. 1384, 140 L.Ed.2d 645 (1998).<sup>FN12</sup> The standard in *Daubert*, however, does not resolve the issue in the present case.<sup>FN13</sup> “*Daubert* is only a threshold inquiry into the admissibility of scientific evidence and other evidentiary rules must also be satisfied.... See [ *State v. Porter*, supra, at 90, 698 A.2d 739].” C. Cwik & J. North, *Scientific Evidence Review: Admissibility and Use of Expert Evidence in the Courtroom* (2003) p. 88. The question presented here goes to the requirement that evidence be reliable so as to satisfy the requirements of the confrontation clause.<sup>FN14</sup> See \*\*934\*797 *State v. Rawls*, 198 Conn. 111, 118, 502 A.2d 374 (1985) (“necessary assurances of reliability” required to satisfy confrontation clause); *Bray v. Bi-State Development Corp.*, 949 S.W.2d 93, 97 (Mo.App.1997) (adequate foundation to authenticate computer generated evidence needed to establish its reliability). The questions regarding the reliability of the evidence in issue in this case look beyond the reliability of the underlying information to whether the evidence had been generated by someone and something that gives the court confidence that the defendant's confrontation rights have been honored. What exactly is required in the context of computer enhanced and computer generated evidence, other than business records, presents an issue of first impression in Connecticut.

FN12. “In [*Porter*] ... we adopted the test for determining the admissibility of scientific evidence set forth in *Daubert* .... We noted

therein two requirements established under *Daubert*. First, that the subject of the testimony must be scientifically valid, meaning that it is scientific knowledge rooted in the methods and procedures of science ... and is more than subjective belief or unsupported speculation.... This requirement establishes a standard of evidentiary reliability ... as, [i]n a case involving scientific evidence, *evidentiary reliability* will be based upon *scientific validity*. ... Second, the scientific evidence must fit the case in which it is presented.... In other words, proposed scientific testimony must be demonstrably relevant to the facts of the particular case in which it is offered, and not simply be valid in the abstract.” (Citations omitted; emphasis in original; internal quotation marks omitted.) *State v. Kirsch*, 263 Conn. 390, 398, 820 A.2d 236 (2003).

FN13. We note that the defendant had filed two motions regarding the bite mark testimony pursuant to *State v. Porter*, supra, 241 Conn. at 57, 698 A.2d 739, but withdrew them for “legal and strategic reasons.” Thus, those aspects of the defendant's appeal concerning the extent to which the evidence should be considered novel “scientific” evidence, and thus subject to the standard enunciated under *Porter*, expressly have been waived.

FN14. On appeal, the defendant argues that bite mark evidence, in general, is unreliable, and that its acceptance as evidence by the judicial system is “controversial.” We disagree. See *State v. Asherman*, 193 Conn. 695, 716, 478 A.2d 227 (1984), cert. denied, 470 U.S. 1050, 105 S.Ct. 1749, 84 L.Ed.2d 814 (1985) (defendant unsuccessfully claimed testimony of odontologist was inadmissible because impossible to discern precise position of victim's scapula at time bite inflicted);

see also *People v. Marx*, 54 Cal.App.3d 100, 107–12, 126 Cal.Rptr. 350 (1975) (defendant unsuccessfully challenged experts' asserted ability to prove identity from similarities between bite marks and dentition of suspected biter); *Bundy v. State*, 455 So.2d 330, 348–49 (Fla.1984) (defendant unsuccessfully argued that act of comparing photographs of bite marks to molds of teeth not reliable or accepted standard of comparison); *Niehaus v. State*, 265 Ind. 655, 660–62, 359 N.E.2d 513 (defendant unsuccessfully argued that odontology not sufficiently recognized as area of expertise and that testifying physician did not qualify as expert in area), cert. denied, 434 U.S. 902, 98 S.Ct. 297, 54 L.Ed.2d 188 (1977); *Commonwealth v. Cifizzari*, 397 Mass. 560, 569, 492 N.E.2d 357 (1986) (defendant unsuccessfully argued that no foundation laid that bite mark identification techniques had gained acceptance in scientific community); *State v. Temple*, 302 N.C. 1, 12, 273 S.E.2d 273 (1981) (defendant unsuccessfully argued that expert witness did not rely on tested methods or proved hypotheses to establish identification of biter).

[3][4] We begin our analysis with the following well established principles. In determining the relevancy and admissibility of evidence, trial courts have broad discretion. *Bovat v. Waterbury*, 258 Conn. 574, 594, 783 A.2d 1001 (2001). “Our standard of review of an evidentiary ruling is dependent on whether the claim is of constitutional magnitude. If the claim is of constitutional magnitude, the state has the burden of proving the constitutional error was harmless beyond a reasonable doubt. *State v. Dehaney*, 261 Conn. 336, 355 n. 12, 803 A.2d 267 (2002), cert. denied, 537 U.S. 1217, 123 S.Ct. 1318, 154 L.Ed.2d 1070 (2003); *State v. Ramos*, 261 Conn. 156, 176, 801 A.2d 788 (2002). Otherwise, in order to establish reversible error on an evidentiary impropriety, the defendant must prove both an abuse of discretion\*798 and a harm that re-

sulted from such abuse. *State v. Young*, 258 Conn. 79, 94–95, 779 A.2d 112 (2001); *State v. Hamilton*, 228 Conn. 234, 244, 636 A.2d 760 (1994).” *State v. Kirsch*, 263 Conn. 390, 412, 820 A.2d 236 (2003).

[5][6] In the present case, the defendant claims that the admission of this evidence without a proper foundation obstructed his constitutional right to confrontation. “The sixth amendment to the constitution of the United States guarantees the right of an accused in a criminal prosecution to be confronted with the witnesses against him. This right is secured for defendants in state criminal proceedings. *Pointer v. Texas*, 380 U.S. 400, 85 S.Ct. 1065, 13 L.Ed.2d 923 (1965). A similar right is embodied in article first, § 8, of the Connecticut constitution. *State v. Hackett*, 182 Conn. 511, 517, 438 A.2d 726 (1980).... [T]he primary interest secured by confrontation is the right of cross-examination. *Davis v. Alaska*, 415 U.S. 308, 315, 94 S.Ct. 1105, 39 L.Ed.2d 347 (1974).” (Internal quotation marks omitted.) *State v. Esposito*, 192 Conn. 166, 178, 471 A.2d 949 (1984). Keeping these principles in mind, we address each type of evidence in turn.

#### A

We first address the admissibility of the computer enhanced photographs of the bite mark. The following additional facts are relevant to our disposition of this issue. At trial, the state presented several images of the bite marks that were computer enhancements of a photograph taken at the victim's autopsy. The enhancements were created through the use of a software program called Lucis. The state introduced the enhancements through Major Timothy Palmbach, overseer of the division of scientific services in the state department of public safety. Palmbach has a master's degree in forensic science, and extensive experience \*799 in the forensic field. Palmbach had obtained the original photographs for the purpose of enhancement from Karazulas. Because the state police did not possess the equipment necessary to generate the digitally enhanced photographs, Palmbach produced the

computer enhanced photographs at Lucis' \*\*935 manufacturer's offices in New Britain, a company called Image Content Technologies. Palmbach explained that Lucis was developed in 1994 specifically for "scientific applications," but that experts had used it in forensic settings.

During his testimony, Palmbach explained how the Lucis program works: "Simply put, what the program will do is it allows us to see image detail that we normally couldn't see otherwise. How it effectively works is it takes advantage ... of the fact that a normal photograph ... has many layers of contrast in it. Your average photograph is going to have around 255 layers of contrast in it. At best our eyes are only capable of perceiving 32 layers of contrast.... So the net result is our eyes see very, very little of actually what's present inside of the image itself. Now, what our eye tends to perceive as far as contrast differences are ... the major contrast differences. We don't have the ability with our own eyes to see the minor contrast differences.... So what this program's intent is ... to allow us to make a selection of a particular range of contrast.... And by ... narrowing [the] band of contrast layers down, we increase the image detail. So we reduce the amount of layers that we're looking at. We're not getting rid of them. We're just saying we only want to look at some of these layers at a particular time.... [T]he result is the picture's got tremendous detail.... At times we end up creating too much detail. We'll get background noise. And it depends upon what it's on. And skin would be a good example. Because if you imagined ... magnifying [and] looking at all the fine detail on your skin—the hairs, the pores, the wrinkles \*800 ... it might actually be very noisy looking. So then ... we'll tell the computer to ... stop showing us quite so much detail."

With the use of a laptop computer, Palmbach demonstrated to the jury exactly how the original bite mark photograph had been enhanced—first by scanning a photograph of the bite mark into the computer,<sup>FN15</sup> then by selecting a particular part of the image to be enhanced, and lastly by defining "contrast

ranges" through the manipulation of a "big cursor" that allows the user to "[diminish] layers" in order to enhance the image's detail, and also through the manipulation of a "small cursor" that allows the user to "reduc[e] the ultrafine detail" in order to dissipate the "noisy effect" of too much detail. Once the cursors are set on certain values, the computer performs an algorithm that engages in a "pixel-to-pixel comparison" in order to enhance the selected image.<sup>FN16</sup> The enhancement produced an image in "one-to-one" format.<sup>FN17</sup> Palmbach testified several times that nothing was added to or removed from the photograph by the enhancement process. Palmbach described how he and Karazulas had "tested" the accuracy of Lucis' enhancement process by taking a photograph of a bite mark that Karazulas \*\*936 \*801 had produced on his own arm, enhancing that photograph, and then comparing the enhancement with the original photograph.

FN15. Palmbach explained that "scanning" an image "changes it from a spatial domain to a frequency domain" whereby the image is converted into pixels. "[A] pixel is the smallest discrete element of an image.... It is a set of bits that represents a graphic image, with each bit or group of bits corresponding to a pixel in the image. The greater the number of pixels per inch, the greater the resolution. A rough analogy to painted art is that a pixel is the same as each colored dab of a pointillist painting." *United States v. Grimes*, 244 F.3d 375, 378 n. 4 (5th Cir.2001).

FN16. Palmbach testified that Lucis' patented algorithm is called "differential hysteresis processing."

FN17. Palmbach testified: "A one-to-one means life-size. It means that the actual image that you would see in the photograph is exactly the same. If we took a picture of my thumb, a one-to-one representation would

mean that we could take a photograph and hold it up to my thumb and it would directly overlay.”

Although much of Palmbach's testimony concerned how the Lucis program worked, he was not qualified as an expert in computer programs, generally, or in Lucis specifically, nor was he qualified as a programmer. Palmbach testified that he was not aware of how the computer makes the distinction as to how many layers there are in an image, or what the algorithm is, or how the algorithm actually sorts the layers. Although he testified that error rates are a cause for concern within the scientific field, he had not seen any published error rates concerning the Lucis program. Additionally, Palmbach testified that Lucis did not create any artifacts in its enhancement process.<sup>FN18</sup>

FN18. Palmbach described an artifact as “an addition. It's an artificial component.... [D]uring the [enhancement] process, the process would create something and do something that was never there to begin with.”

[7] The defendant objected to the admission of the enhanced photographs, arguing that Palmbach's testimony laid an inadequate foundation. The trial court overruled that objection. On appeal, the defendant argues that the evidence at issue resembles composite photographs, and therefore, should be governed under a similar standard. With respect to composite photographs, “[t]he moving party must present witnesses with firsthand knowledge of how the composite was prepared and of how accurately it portrays that which it is intended to depict.” *State v. Weidenhof*, 205 Conn. 262, 275, 533 A.2d 545 (1987).<sup>FN19</sup> The defendant also claims that because this evidence actually was created \*802 by and through the use of a computer, it is computer generated evidence, and thus entails additional foundational requirements.

FN19. The state, while doubting the appropriateness of the analogy to composite photographs, claims that this foundational standard was met. See *State v. Packard*, 184 Conn. 258, 274, 439 A.2d 983 (1981) (stating that testimony of police officer who helped victim create composite was no more necessary as condition of admissibility than photographer's testimony would have been had victim identified photograph).

[8][9][10][11] The state argues, to the contrary, that the Lucis enhanced photographs are mere “reproductions” of the photograph of the bite mark, and that their admissibility therefore should be governed by the foundational standard for photographs. Under that standard, all that is required is that a photograph be introduced through a witness competent to verify it as a fair and accurate representation of what it depicts.<sup>FN20</sup> See \*\*937*State v. DeForge*, 194 Conn. 392, 397, 480 A.2d 547 (1984); *Cagianello v. Hartford*, 135 Conn. 473, 475, 66 A.2d 83 (1948). The state argues that the enhancements met this burden because the authenticity of the original photographs was never questioned and the testimony at trial was that the enhancements accurately reflected the content of the originals. The state further argues that a photographer's in-court testimony is not required for the admission of a photograph; see *McGar v. Bristol*, 71 Conn. 652, 655, 42 A. 1000 (1899); and therefore, the computer programmer's testimony is not required in this instance.

FN20. Although the state properly identifies the standard for admitting demonstrative evidence; see C. Tait, *Connecticut Evidence* (3d Ed. 2001) § 11.15.1, pp. 810–11; it nevertheless labels the enhanced photographs and the computer generated overlays as merely “illustrative evidence,” and argues that, as such, they may be admitted “if, in the opinion of the trial court, it will assist the jury in understanding an expert's testimony.”

(Internal quotation marks omitted.) *State v. Dontigney*, 215 Conn. 646, 652, 577 A.2d 1032 (1990). The state claims that the photographs and overlays served simply to explain or demonstrate the testimony of Karazulas, the forensic odontologist, but did not themselves constitute evidence. We do not agree with the state's characterization. The record reveals that these items were admitted as evidence, and as such, constitute demonstrative evidence. "Demonstrative evidence is a pictorial or representational communication incorporated into a witness's testimony.... However, demonstrative evidence is not merely 'illustrative'; it is just as much substantive evidence of the facts it depicts or portrays as is real or testimonial evidence. *Tarquinio v. Diglio*, 175 Conn. 97, 98, 394 A.2d 198 (1978)." (Citation omitted.) C. Tait, *supra*, at § 11.1, pp. 796–97.

**\*803** We note first that there is some question as to whether what is at issue here is actually computer generated evidence. Currently, there is no universal definition of that term; many commentators, however, and some courts, divide computer generated evidence into two distinct categories of evidence: simulations and animations. "In a simulation, data is entered into a computer which is programmed to analyze the information and perform calculations by applying mathematical models, laws of physics and other scientific principles in order to draw conclusions and recreate an incident.... In contrast, an animation does not develop any opinions or perform any scientific calculations and, to the contrary, is nothing more than a graphic depiction or illustration of the previously formed opinion of an expert." (Citations omitted.) *Commonwealth v. Serge*, 58 Pa. D. & C.4th 52, 68–69 (2001). The evidence at issue in the present case does not fall cleanly within either category,<sup>FN21</sup> but we determine it to be more than the mere "enlargement"<sup>FN22</sup> of a photograph, as the state argues. **\*804** Enlargement simply involves making the details of an image larger,

whereas the enhancement process in this case "reveals" parts of an image that previously were unviewable.<sup>FN23</sup>

FN21. At this time, we reserve judgment on the validity of these two categories of computer generated evidence, as such, and withhold our agreement as to the merits of this bifurcated approach.

FN22. "Enlargement is simply a multiplication process. An enlargement merely increases the size of the image.... Enhancement differs from ... enlargement.... Image enhancement is a subtractive process, which improves image contrast by removing interfering colors and background patterns.... [I]mage enhancement technology poses a problem in the validation of the underlying scientific process.

"Image enhancement technology was developed during the late 1960s and early 1970s for the [National Aeronautics and Space Administration (NASA)] space program.... Due to the weight and power limitations of spacecraft, it was impractical for NASA to use state-of-the-art camera systems on unmanned craft. The cameras used produced somewhat degraded photographs. Image enhancement reverses the degradation ... and thereby improve[s] the sharpness and image contrast of the photograph ... [by] eliminat[ing] background patterns and colors." (Internal quotation marks omitted.) 2 P. Giannelli & E. Imwinkelried, *Scientific Evidence* (3d Ed. 1999 & Sup. 2003) § 25–6.1, pp. 92–93; see also *State v. Hayden*, 90 Wash.App. 100, 105, 950 P.2d 1024 (1998) ("the technology used to enhance photographs of latent prints evolved from jet propulsion laboratories in the NASA space program to

isolate galaxies and receive signals from satellites”).

FN23. The state argues that Palmbach's testimony at trial revealed that the Lucis program does not “add” or “subtract” any details from an image, but merely presents a limited number of “contrast layers” from which to view—that it does not “change” the image, but merely “focuses” on one part of the image rather than another. What is obvious, however, and what Palmbach confirmed, is that the Lucis program reveals details to the human eye that were not visible before the enhancement. We conclude that, simply put, the program actually is “creating” some part of the image, to the extent that it reveals that which was not visible before. Therefore, it is different from a mere enlargement.

**\*\*938** Our research reveals that, of the few cases that actually discuss the admission of computer enhanced evidence, none explicitly qualifies such evidence as “computer generated.” See, e.g., *United States v. Calderin-Rodriguez*, 244 F.3d 977, 986 (8th Cir.2001) (digitally enhanced sound recordings); *Nooner v. State*, 322 Ark. 87, 103–104, 907 S.W.2d 677 (1995) (digitally enhanced videotape), cert. denied, 517 U.S. 1143, 116 S.Ct. 1436, 134 L.Ed.2d 558 (1996); *Dolan v. State*, 743 So.2d 544, 545–46 (Fla.App.1999) (same); *English v. State*, 205 Ga.App. 599, 599–600, 422 S.E.2d 924 (1992) (same); *State v. Hayden*, 90 Wash.App. 100, 103, 950 P.2d 1024 (1998) (digitally enhanced fingerprint). We note, however, that the appearance of computer generated evidence in our courts is becoming more common. Not only can we not anticipate what forms this evidence will take, but also common sense dictates that the line between one type of computer generated evidence and another will not always be obvious.

[12] Therefore, because in the present case, we cannot be sure to what extent the difference between

presenting evidence and creating evidence was blurred, we let caution guide our decision. We do not agree with the state's proposition that the enhanced photographs in \*805 the present case are like any other photographs admitted into evidence,<sup>FN24</sup> and we determine that, to the extent that a computer was both the process and the tool used to enable the enhanced photographs to be admitted as evidence, we consider these exhibits, for the purposes of this analysis, to be computer generated.

FN24. Specifically, the original photographs of the bite mark were digitized. We note that “[d]igital images are easier to manipulate than traditional photographs and digital manipulation is more difficult to detect.” J. Witkowski, “Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images,” 10 Wash. U. J.L. & Policy 267, 271 (2002). After the photographs were put in a digital format, they were enhanced, a process which can also introduce manipulation or alteration of the original image. See M. Cherry, “Reasons to Challenge Digital Evidence and Electronic Photography,” 27 Champion 42, 42–43 (2003). We note further that, unlike other types of enhancement wherein the original and the enhanced product could easily be inspected visually for distortion, or dissimilarity, the images in this case involve a bite mark, which, because it actually is composed of multiple smaller marks, is not so easily inspected. Odontological matching depends on millimeters. A visual inspection of the unenhanced and enhanced photographs alone, therefore, is not enough to ensure the enhancement's reliability because this particular forensic analysis involves the subtle discernment of infinitesimal differences. Other types of enhanced evidence, such as videotapes, may be more amenable to visual inspection because they are larger in scale.

The appearance of computer generated evidence in Connecticut cases is limited. For the most part, cases in Connecticut that give rise to the question of the admissibility of computer generated evidence involve the admissibility of computerized business records. *American Oil Co. v. Valenti*, 179 Conn. 349, 360, 426 A.2d 305 (1979); *Midstates Resources Corp. v. Dobrindt*, 70 Conn.App. 420, 426, 798 A.2d 494 (2002); *Ninth RMA Partners, L.P. v. Krass*, 57 Conn.App. 1, 9–11, 746 A.2d 826, cert. denied, 253 Conn. 918, 755 A.2d 215 (2000); *Federal Deposit Ins. Corp. v. Carabetta*, 55 Conn.App. 369, 376–77, 739 A.2d 301, cert. denied, 251 Conn. 927, 742 A.2d 362 (1999); *State v. Dumas*, 54 Conn.App. 780, 797–98, 739 A.2d 1251, cert. denied, 252 Conn. 903, 743 A.2d 616 (1999); *\*806Farmers & Mechanics Bank v. Krupa*, 52 Conn.App. 493, 495, 727 A.2d 252 (1999); *Webster Bank v. Flanagan*, 51 Conn.App. 733, 744–48, 725 A.2d 975 (1999); *SKW Real Estate Ltd. Partnership v. Gallicchio*, 49 Conn.App. 563, 575–78, 716 A.2d 903, cert. denied, *\*\*939247* Conn. 926, 719 A.2d 1169 (1998); *Berkeley Federal Bank & Trust, FSB v. Ogalin*, 48 Conn.App. 205, 207–11, 708 A.2d 620, cert. denied, 244 Conn. 933, 711 A.2d 726 (1998); *State v. Capriozzi*, 45 Conn.App. 455, 458–61, 696 A.2d 380, cert. denied, 243 Conn. 937, 702 A.2d 644 (1997); *Shadhali, Inc. v. Hintlian*, 41 Conn.App. 225, 227–29, 675 A.2d 3, cert. denied, 237 Conn. 926, 677 A.2d 948 (1996); *Shawmut Bank Connecticut, N.A. v. Connecticut Limousine Service, Inc.*, 40 Conn.App. 268, 275–77, 670 A.2d 880, cert. denied, 236 Conn. 915, 673 A.2d 1143 (1996); *Babiarz v. Hartford Special, Inc.*, 2 Conn.App. 388, 397–98, 480 A.2d 561 (1984); c.f. *State v. Polanco*, 69 Conn.App. 169, 184, 797 A.2d 523 (2002) (computer generated map admitted under testimony by geographic information systems technician verifying accuracy of program and result); *State v. Wright*, 58 Conn.App. 136, 148–49, 752 A.2d 1147, cert. denied, 254 Conn. 907, 755 A.2d 884 (2000) (same).

In the seminal case of *American Oil Co. v.*

*Valenti*, supra, 179 Conn. at 359, 426 A.2d 305, wherein this court first addressed the standard to be used in admitting computer generated evidence, the court adopted a general rule, requiring “testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer.” In that case, the court cautioned, “[c]omputer machinery may make errors because of malfunctioning of the hardware, the computer’s mechanical apparatus. Computers may also, and more frequently, make errors that arise out of defects in the software, the input procedures, the data base, and the processing program.... In view of the complex *\*807* nature of the operation of computers and general lay unfamiliarity with their operation, courts have been cautioned to take special care to be certain that the foundation is sufficient to warrant a finding of trustworthiness and that the opposing party has full opportunity to inquire into the process by which information is fed into the computer.” (Citations omitted; internal quotation marks omitted.) *Id.*, at 358–59, 426 A.2d 305.

In *American Oil Co.*, the court did not require the computer programmer, or even the person who had entered the information into the computer, to testify, because the reliability of the records was extrinsically established. *Id.*, at 360–61, 426 A.2d 305. “Routinely prepared records ... are well recognized exceptions to the hearsay rule, because their regular use in the business of the company insures a high degree of accuracy. Proof of day-to-day business reliance upon computerized records should therefore make less onerous the burden of laying a proper foundation for their admission.” *Perma Research & Development Co. v. Singer Co.*, 542 F.2d 111, 125 (2d Cir.) (Van Graafeiland, J., dissenting), cert. denied, 429 U.S. 987, 97 S.Ct. 507, 50 L.Ed.2d 598 (1976). In the case before us, such reliability has not been extrinsically established, and therefore, the standard in *American Oil Co.*, although a good starting place, provides only limited guidance. We therefore find it necessary to look outside our jurisdiction to further refine the ap-

propriate foundational requirements for computer generated or computer enhanced evidence that does not constitute business records.

Although computer enhanced photographs, and the like, have surfaced as evidence in recent cases, both in Connecticut and elsewhere, their admissibility apparently has not been challenged on a basic foundational \*808 issue such as in the present case.<sup>FN25</sup> See, e.g., \*\*940 *State v. Asherman*, 193 Conn. 695, 717, 478 A.2d 227 (1984) (odontologist used life-sized enlargements and creation of “mirror image” photograph of defendant's teeth by photographing defendant's teeth and taking special scan photographs inside defendant's mouth), cert. denied, 470 U.S. 1050, 105 S.Ct. 1749, 84 L.Ed.2d 814 (1985); *Bundy v. State*, 455 So.2d 330, 336–37 (Fla.1984) (one forensic dental expert used enlarged photographs, another used computer enhanced photographs). We note, however, that similar computer enhancement has been discussed in the context of other types of evidence. For example, images from videotapes have been enhanced for evidentiary purposes. Those jurisdictions addressing the issue of enhancement in the context of videotape have permitted such enhancements as evidence, and we find these cases instructive.<sup>FN26</sup>

FN25. Commentators have attempted to explain this lack of case law involving basic foundational challenges to this sort of evidence. “Although computer systems raise serious reliability issues, the reported cases do not adequately reflect this reality.” R. Garcia, “‘Garbage In, Gospel Out’: Criminal Discovery, Computer Reliability, and the Constitution,” 38 UCLA L. Rev. 1043, 1087 (1991). “Why do the reported cases fail to adequately expose the serious reliability issues raised by computerized information? Many people, including defense attorneys, prosecutors, judges, and juries, do not understand computers. As a result, people tend

to suspend their healthy common sense skepticism when they deal with information technology. Computers make it possible to do some things that could not be done without computers. The mere fact that computers can do some things at all tends to mask the issue of whether the computers can do it well. The ‘gee whiz’ quality of computers may conceal the underlying frailties of the systems.” *Id.*, at 1090.

FN26. We note that the digital enhancement of evidence has been accepted in the courtroom in other contexts as well. For example, in a case involving the digital enhancement of fingerprint evidence, a forensic analyst took digital images of pieces of a bloody sheet and then “utilized computer software to filter out background patterns and colors to enhance the images so that the prints could be viewed without the background patterns and colors.” *State v. Hayden*, supra, 90 Wash.App. at 103, 950 P.2d 1024. *Hayden*, however, did not involve the basic issue of adequate foundation, and instead involved an analysis under the standard for “novel scientific evidence” laid out in *Frye v. United States*, 293 F. 1013 (D.C.Cir.1923). In *Hayden*, the court held that enhanced digital imaging process generally was accepted in the relevant scientific community “[b]ecause there does not appear to be a significant dispute among qualified experts as to the validity of enhanced digital imaging performed by qualified experts using appropriate software. ...” (Emphasis in original.) *State v. Hayden*, supra, at 109, 950 P.2d 1024. The court also noted that the technique utilized by the forensic analyst “ha[d] a reliability factor of 100 percent and a zero percent margin of error and that the results are visually verifiable and could be easily duplicated by another expert using his or her own digital camera

and appropriate computer software.” Id.

\*809 In *Nooner v. State*, supra, 322 Ark. at 104, 907 S.W.2d 677, the Arkansas Supreme Court upheld a ruling in a pretrial hearing that “so long as the process leading to the duplicate videotape and enhanced photographs was explained to the jury,” they could be introduced as evidence. Stating that “[r]eliability must be the watchword in determining the admissibility of enhanced videotapes and photographs, whether by computer or otherwise,” the court allowed the enhancements because their reliability was attested to by multiple witnesses who all “meticulously described their role in the enhancement process.” Id. Witnesses in *Nooner* included the person who “slowed” down the videotape enough to make still photographs from it; the person who took a still photograph from the videotape, transferred it to his computer, softened the pixels to remove graininess, and then placed the resulting image on a computer disk; and the person who took the computer disk and printed still photographs, including a photograph in which he had “multiplied the pixels per square inch to improve the contrast and adjusted the brightness in one of the still photographs.” Id. Additionally, \*\*941 the court noted that there was no evidence of distortion in the enhancements, nor was there any evidence to indicate that the enhancement somehow had changed a face, features, or physique, or had been altered to include someone or something not present on the videotape. Id.

Similarly, in *English v. State*, supra, 205 Ga.App. 599, 422 S.E.2d 924, the Georgia Court of Appeals, analogizing the admissibility of a computer enhanced videotape to photographic\*810 enlargements,<sup>FN27</sup> admitted the videotape when the technician who performed the enhancement testified to the process and further testified that the photographic copy, as enhanced, was a “‘fair and accurate’” representation of what appeared in the frozen frames of the videotape copy. In *Dolan v. State*, supra, 743 So.2d at 546, the Florida District Court of Appeal allowed the admission of enhanced still prints wherein it was established

that the original videotape from which they were taken accurately reflected the store in which a sexual battery occurred when “there [was] testimony as to the nature of the store’s video security system, the placement of the film in the camera, [and] how the camera worked,” and a forensic analyst “explain[ed] the computer enhancement process and establish [ed] that the images were not altered or edited....”

FN27. We find *English* to be instructive on the issue although we do not agree with the court’s direct analogy of computer enhancements to photographic enlargements.

What is consistent, in all three cases, is that the technician or analyst who testified was the person who had engaged in the enhancement process and was capable of testifying in specific detail as to the process. See *Nooner v. State*, supra, 322 Ark. at 104, 907 S.W.2d 677; *Dolan v. State*, supra, 743 So.2d at 546; *English v. State*, supra, 205 Ga.App. 599, 422 S.E.2d 924. This is consistent with this court’s ruling in *American Oil Co.* that, in order for computer generated evidence to be admitted, there must be “testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer.” *American Oil Co. v. Valenti*, supra, 179 Conn. at 359, 426 A.2d 305. Contrary to the defendant’s assertions in the present case, however, this standard does not dictate that the *only* person capable of such expertise is the programmer of the software.

\*811 As we have in the past, we look to the federal rules for further guidance on this issue. See, e.g., *State v. Weinberg*, 215 Conn. 231, 242–43, 575 A.2d 1003 (relying on rule 601 of Federal Rules of Evidence), cert. denied, 498 U.S. 967, 111 S.Ct. 430, 112 L.Ed.2d 413 (1990); *Mac’s Car City, Inc. v. American National Bank*, 205 Conn. 255, 260–61, 532 A.2d 1302 (1987) (relying on rules 54[b] and 56[f] of Federal Rules of Civil Procedure); *State v. Nardini*, 187 Conn. 513, 526, 447 A.2d 396 (1982) (relying on

rule 609[b] of Federal Rules of Evidence). Rule 901(b)(9) of the Federal Rules of Evidence provides that authentication or identification of a process or system requires “[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.” The advisory committee notes to rule 901(b)(9) <sup>FN28</sup> provide that the rule “is designed for situations in which the accuracy of a result is dependent upon a process or system which produces it.” The notes also suggest that the rule is particularly adapted to such “recent developments” as the computer. Therefore, the federal rule dictates that **\*\*942** the inquiry into basic foundational admissibility requires sufficient evidence to authenticate both the accuracy of the image *and* the reliability of the machine producing the image.

FN28. We note that rule 901 of the Federal Rules of Evidence is consistent with § 9–1(a) of the Connecticut Code of Evidence, except that rule 901(b) contains an additional list of illustrations.

[13] Several factors that establish authentication under rule 901 of the Federal Rules of Evidence have been identified. “This standard can generally be satisfied by evidence that (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 information, (4) a reliable software program was utilized, (5) the equipment **\*812** was programmed and operated correctly, and (6) the exhibit is properly identified as the output in question.” C. Mueller & L. Kirkpatrick, *Evidence: Practice Under the Rules* (2d Ed. 1999) § 9.16, p. 1442 (citing other commentators); E. Weinreb, “ ‘Counselor, Proceed With Caution’: The Use of Integrated Evidence Presentation Systems and Computer-Generated Evidence in the Courtroom,” 23 Cardozo L. Rev. 393, 410 (2001) (citing same factors); see *Commercial Union Ins. Co. v. Boston Edison Co.*, 412 Mass. 545, 549, 591 N.E.2d

165 (1992) (conditioning admissibility on sufficient showing that: “[1] the computer is functioning properly; [2] the input and underlying equations are sufficiently complete and accurate [and disclosed to the opposing party, so that they may challenge them]; and [3] the program is generally accepted by the appropriate community of scientists”); *Kudlacek v. Fiat S.p.A.*, 244 Neb. 822, 843, 509 N.W.2d 603 (1994) (same); *State v. Clark*, 101 Ohio App.3d 389, 416, 655 N.E.2d 795 (1995) (same), *aff’d*, 75 Ohio St.3d 412, 662 N.E.2d 362 (1996); *Clark v. Cantrell*, 339 S.C. 369, 384, 529 S.E.2d 528 (2000) (holding computer generated evidence admissible where it is [1] authentic under state equivalent to federal rule 901[b][9], [2] relevant under state evidence rules, [3] a “fair and accurate representation of the evidence to which it relates” and [4] its probative value substantially outweighs dangers of its admission); see also *Bray v. Bi-State Development Corp.*, *supra*, 949 S.W.2d at 97–100 (noting that three guidelines for admissibility established in *Commercial Union Ins. Co.* as well as rule 901[b][9] of Federal Rules of Evidence provide “helpful starting point” but not adopting strict formula or set of guidelines).

[14][15][16] We agree that “[r]eliability must be the watchword” in determining the admissibility of computer generated evidence; *Nooner v. State*, *supra*, 322 Ark. at 104, 907 S.W.2d 677; and we conclude that these six factors adequately refine our **\*813** requirement enunciated in *American Oil Co.* that, in order to lay a proper foundation for computer generated evidence, there must be “testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer.” *American Oil Co. v. Valenti*, *supra*, 179 Conn. at 359, 426 A.2d 305. In addition to the reliability of the evidence itself, what must be established is the reliability of the procedures involved, as defense counsel must have the opportunity to cross-examine the witness as to the methods used. We note that “[r]eliability problems may arise through or in: (1) the underlying

information itself; (2) entering the information into the computer; (3) the computer hardware; (4) the computer software (the programs or instructions that tell the computer what to do); (5) the execution of the instructions, which transforms the information in some way—for example, by calculating numbers, sorting names, or storing information and retrieving it later; (6) the output (the information as produced by the computer in \*\*943 a useful form, such as a printout of tax return information, a transcript of a recorded conversation, or an animated graphics simulation); (7) the security system that is used to control access to the computer; and (8) user errors, which may arise at any stage.” R. Garcia, “ ‘Garbage In, Gospel Out’: Criminal Discovery, Computer Reliability, and the Constitution,” 38 UCLA L. Rev. 1043, 1073 (1991); see also K. Butera, “Seeing is Believing: A Practitioner’s Guide to the Admissibility of Demonstrative Computer Evidence,” 46 Clev. St. L. Rev. 511, 525 (1998) (proper authentication requires that reliability of computer process and accuracy of results be subject to scrutiny).

[17] We believe that these factors effectively address a witness’ familiarity with the type of evidence and with the method used to create it, and appropriately require that the witness be acquainted with the technology \*814 involved in the computer program that was used to generate the evidence. These factors also ensure that the hardware and software used to generate the evidence were adequate for that purpose and that the technology was reliable. As in our decision in *Porter*, we stress that these factors represent an approach to the admissibility of computer generated evidence, and not a mechanical, clearly defined test with a finite list of factors to consider. See *State v. Porter*, supra, 241 Conn. at 79, 698 A.2d 739. “Trial courts must have considerable latitude in determining the admissibility of evidence in this area as in others.” *American Oil Co. v. Valenti*, supra, 179 Conn. at 360, 426 A.2d 305. Although a trial court should weigh and balance these factors and decide whether they ultimately support the admissibility of the evidence, we

offer these factors to serve as guideposts, and do not suggest that these factors necessarily are to be held in equipoise. See *Bray v. Bi-State Development Corp.*, supra, 949 S.W.2d at 99 (“Few jurisdictions have attempted to enunciate a formula or fixed set of guidelines to govern the establishment of a foundation for computer-generated evidence other than business records. However, there is a developing consensus ... which agrees on how the accuracy of computer-generated evidence can be established and gives a trial court sufficient parameters to exercise its discretion in this area without the need for a precise formula.”).

[18] Applying these factors to the facts of the present case, we conclude that the state laid an adequate foundation for the Lucis enhancements of the bite mark photograph. First, Palmbach testified that the computer equipment is accepted as standard equipment in the field.<sup>FN29</sup> He testified that the Lucis program was relied \*815 upon by experts in the field of pattern analysis in a forensic setting. He further testified that the program had been used in “fingerprint pattern identification, bloodstain pattern identification, footwear and tire impression identification, and in bite mark identification.” Second, it was established that a qualified computer operator produced the enhancement. Palmbach’s testimony clearly demonstrated that he was well versed in the Lucis program. He was a well trained and highly experienced forensic analyst, and he testified to his qualifications as an expert in the analysis of pattern evidence and the enhancement of that evidence. Palmbach testified on cross-examination that he previously had created digitally enhanced images of footprints and tire prints, and that on two \*\*944 occasions, he had created digitally enhanced images of dental imprints on breasts. Additionally, Karazulas, an odontological expert, was with Palmbach throughout the process and was able to aid him in determining when the image was appropriately enhanced for forensic comparison. Contrary to the defendant’s assertion, there is no evidence in the record that Barbara Williams, the president and chief

executive officer of the company that manufactured the Lucis program; see footnote 29 of this opinion; actually participated in the enhancement, or that Palmbach relied on her expertise to produce a properly enhanced image. Rather, the record reveals that Palmbach and Williams merely had “discussions.” As the trial court stated in overruling the defendant’s objection to the admissibility of the evidence, “[t]he process at all times was under the control of [Palmbach].”

FN29. Originally, the Lucis enhancement was accomplished using the state’s computer equipment, but the actual evidence at issue was produced by Palmbach at the office of Image Content Technology, LLC, which manufactured the Lucis program, because it had a high resolution scanner and printer.

Third, the state presented evidence that proper procedures were followed in connection with the input and output of information. During direct examination, Palmbach testified accurately, clearly, and consistently regarding the process of the digitization of the image—wherein a photograph is transformed into pixels; see \*816 footnote 15 of this opinion;—and how Palmbach then had used the Lucis software to select comparable points of contrast and array them into layers. He also testified as to how the Lucis program then diminished certain layers in order to heighten the visual appearance of the bite mark. During voir dire and cross-examination, Palmbach further explained and clarified this process. In fact, he even demonstrated the enhancement process to the jury using a laptop demonstration. Importantly, Palmbach compared the enhanced photographs with the unenhanced photographs in front of the jury. When asked whether there was anything in the enhanced image that was not present in the original image, Palmbach testified: “No ... there’s not. One of the features of Lucis is that it does not remove any pixels. It is only selecting to show you the range that you’ve asked for. Every one of those pictures and every bit of

that contrast is still present in the enhanced portion.... It’s just that we’re diminishing some and bringing others forward ... just for viewing purposes. But every bit of that information is still present. We have not selected out or deleted some of these pixels or any of the pixels.”

Fourth, the state adequately demonstrated that Lucis is a reliable software program. Palmbach testified that, in a forensic setting, the “primary concern is accuracy.... [W]e can’t choose a program in which it will delete, alter, or change that material in any form or fashion. If it does, it’s not suitable for this type of analysis.” He further testified that the Lucis program, unlike other computer programs such as Adobe Photoshop, does not even have image editing features and was not designed to edit the images it enhances. Therefore, the defendant’s concern that the computer edited or distorted the image is misplaced. Although Palmbach testified that he was not aware of the error rates regarding the Lucis program, he stated that he was aware of Lucis’ marketing papers and an article that had been written \*817 concerning Lucis, both of which claimed that the program was artifact free, which would contribute greatly to a low error rate. Additionally, Palmbach personally tested Lucis’ accuracy by making a known exemplar using a bite mark made by Karazulas on his own arm and then subjecting it to enhancement.

Our review of the record through the lens of the previously enunciated factors reveals that the state presented testimony that sufficiently established the reliability of the evidence and the processes that produced it. Although Palmbach admitted that the algorithm itself was programmed \*\*945 by someone who “knows a lot more about computers” than he did, our review of the record reveals that Palmbach had sufficient knowledge of the processes involved in the enhancement to lay a proper foundation.

As we previously have mentioned, some commentators and courts divide computer generated evi-

dence into separate categories of animation and simulation. It has been suggested that these categories determine which evidentiary foundation should govern the admissibility of the evidence. See *Commonwealth v. Serge*, supra, 58 Pa. D. & C.4th at 71 (citing cases and commentary).<sup>FN30</sup> We repeat, however, that, at least in the present \*818 case, we do not find these categories to be helpful.<sup>FN31</sup> Nor do we agree with commentary that suggests that application of the same standard to all types of computer generated evidence, without differentiation, will cause mischief. See F. Galves, “Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance,” 13 Harv. J.L. & Tech. 161, 256 (2000) (stressing importance of applying different standards of admissibility to animations and simulations because animations are illustrative evidence and thus should have lower threshold for admissibility than simulations admitted as substantive evidence). Instead, we see no harm in applying a single standard, one that is fairly stringent and uses reliability as its touchstone. As the presence and use of computer generated evidence in courtrooms increases, so will our understanding of its attendant processes. The drafters of rule 901 of the Federal Rules of Evidence recognized this potential familiarity with what today seems like nascent technology. The advisory committee notes to rule 901 provide that: “[r]ule 901(b)(9) does not, of course, foreclose taking judicial notice of the accuracy of the process or system.” We believe that there is no harm in requiring the courts of this state to take the time to ensure that basic foundational requirements \*819 are met, particularly because the potential mischief<sup>FN32</sup> \*\*946 caused by a standard that is too lax would be great.<sup>FN33</sup>

FN30. Courts that follow such an approach explain that an animation is only illustrative evidence, and thus should have a lower threshold for admissibility than do simulations, which are received as substantive evidence. Compare *Commercial Union Ins. Co.*

*v. Boston Edison Co.*, supra, 412 Mass. at 549, 591 N.E.2d 165 (simulation), *Kudlacek v. Fiat S.p.A.*, supra, 244 Neb. at 843, 509 N.W.2d 603 (same), and *State v. Clark*, supra, 101 Ohio App.3d at 416–17, 655 N.E.2d 795 (same) with *Pierce v. State*, 718 So.2d 806, 808 (Fla.App.1997) (animation), *Cleveland v. Bryant*, 236 Ga.App. 459, 460, 512 S.E.2d 360 (1999) (same), *Harris v. State*, 13 P.3d 489, 495 (Okla.Crim.App.2000) (same), cert. denied, 532 U.S. 1025, 121 S.Ct. 1971, 149 L.Ed.2d 764 (2001), and *Mintun v. State*, 966 P.2d 954, 959 (Wyo.1998) (same); see also F. Galves, “Where the Not So Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance,” 13 Harv. J.L. & Tech. 161, 227–30 (2000) (comparing differing admission standards for animations and simulations); E. Weinreb, supra, at 23 Cardozo L. Rev. 403–404; 2 P. Giannelli & E. Imwinkelried, *Scientific Evidence* (3d Ed. 1999 & Sup. 2002) § 25–6, pp. 69–71 (citing cases); 2 C. McCormick, *Evidence* (5th Ed. 1999 & Sup. 2003) § 214, p. 2 (“[c]omputer generated evidence used solely to illustrate testimony is commonly denominated an ‘animation,’ while computer models purporting to recreate the event in question are termed ‘simulations’”).

FN31. We further point out that the reasoning utilized in cases distinguishing simulations and animations is not applicable in the present case in light of the fact that the Adobe Photoshop superimpositions, which most closely resemble animations, actually were used as substantive, not merely illustrative, evidence.

FN32. We are cognizant of the strong impact

that computer generated evidence may have on juries. “Part of the mystique of computers is the aura of reliability that computers share with other forms of scientific and technical evidence. The impact that scientific evidence has on juries has been an issue in the criminal justice system for some time and in various contexts.... As one juror explained after a recent trial, ‘You can’t argue with science.’ ” R. Garcia, *supra*, at 38 UCLA L. Rev. 1091.

FN33. We are not the first court to be concerned with the reliability of computer generated evidence. “As courts are drawn willy-nilly into the magic world of computerization, it is of utmost importance that appropriate standards be set for the introduction of computerized evidence. Statements ... that a computer is but [a calculator] ... with a giant memory ... represent an overly-simplified approach to the problem of computerized proof which should not receive this Court’s approval. Although the computer has tremendous potential for improving our system of justice by generating more meaningful evidence than was previously available, it presents a real danger of being the vehicle of introducing erroneous, misleading, or unreliable evidence.... Because of the complexities of examining the creation of computer-generated evidence and the deceptively neat package in which the computer can display its work product, courts and practitioners must exercise more care with computer-generated evidence than with evidence generated by more traditional means.” (Internal quotation marks omitted.) *Perma Research & Development Co. v. Singer Co.*, *supra*, 542 F.2d at 124–25 (Van Graafeiland, J., dissenting); accord *United States v. De Georgia*, 420 F.2d 889, 895–96 (9th Cir.1969) (Ely, J., concurring); *Commonwealth v. Klinghoffer*, 522 Pa. 562, 569, 564

A.2d 1240 (1989) (Larsen, J., dissenting).

Our research reveals that such an approach has echoes in distant jurisprudence. In the earliest cases that admitted sound recordings, video recordings, and even photographs, courts had strict admissibility requirements, but later relaxed these requirements as the technology involved gained greater acceptance with its consistent use. See J. Witkowski, “Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images,” 10 Wash. U. J.L. & Policy 267, 276–80 (2002) (citing cases); see also *Cunningham v. Fair Haven & Westville R. Co.*, 72 Conn. 244, 250, 43 A. 1047 (1899) (“[i]t is common knowledge that as to such matters, either through want of skill on the part of the artist, or inadequate instruments\*820 or materials, or through intentional and skillful manipulation, a photograph may be not only inaccurate but dangerously misleading”); *Dyson v. New York & New England R.R. Co.*, 57 Conn. 9, 24, 17 A. 137 (1888) (offer of photographs accompanied by testimony of photographer who took them as to their accuracy, and of surveyor who identified points of view). Like the photograph, even the most advanced technologies today will seem commonplace tomorrow. Importantly, the factors we enunciate in this opinion provide for both circumstances. Moreover, we note that, because the domain of computer generated evidence expands on a nearly daily basis, by the time we could make a ruling regarding one particular program or application, that program would become obsolete and a new one would take its place. We do not wish to enunciate a standard that is applicable today and useless tomorrow.

## B

We next address the admissibility of the exhibits created with Adobe Photoshop. The following additional facts are relevant to the disposition of this issue. Through Karazulas, the state offered overlays, created with the use of Adobe Photoshop, which superimposed images of the defendant’s dentition over photographs of the bite mark.<sup>FN34</sup> Karazulas had extensive

**\*\*947** training and experience in the study of bite mark identification, and was admitted as an expert in the field of forensic odontology. **\*821** He testified that bite mark identification is based upon the recognition of unique characteristics of the person whose teeth had left that mark. He further testified that different teeth leave varying marks; for example, incisors leave rectangular marks while cuspids leave pointed or triangular marks.

FN34. The photograph of the victim's left breast actually revealed two separate bite marks. Karazulas explained that all tests and observations were conducted on the inner bite mark—the one closest to the nipple. Karazulas testified that, although the outer bite mark was consistent with the inner one, it was more difficult to match the models of the teeth to the outer mark because it was made on an area with a larger circumference. He explained that, with compression of a large area that is soft and curved, like breast tissue, when the pressure is released, the mark expands beyond the point where it was compressed. Karazulas further testified that, with reasonable medical certainty, the same teeth had made both marks on the victim's breast.

In the process of coming to the conclusion that the defendant was the biter, Karazulas employed a number of comparative techniques. First, Karazulas examined the molds made from the defendant's teeth. He testified that, from these molds, he could discern several unique characteristics. In the upper left side of the mouth, the left upper cuspid was rotated instead of being flush to the other teeth, and the cuspid on the other side was also rotated. The upper left central and lateral incisors also were tipped forward. On the lower jaw, Karazulas pointed out that there were spaces behind several teeth—on the lower left between the cuspid and bicuspid, on the lower right between the cuspid and the lateral incisor, and between the right

cuspid and the first bicuspid. He further pointed out that, “[a]s you look at the arch, it slants up to the right. All the teeth move upward and to the right.”

Next, Karazulas examined unenhanced photographs of the bite mark. Looking at these, Karazulas could tell by their orientation that the marks had been inflicted by someone standing directly in front of the victim and approaching her breast in a head-on position. By the shape, circumference, size and individual characteristics of the bite marks, he could tell that the marks above the nipple had been made by the upper jaw, or maxillary teeth, and the marks under the nipple had been made by the mandibular teeth. With regard to the photographs, Karazulas stated that their quality was “excellent,” and that he could see the circumference of the arch, the individual characteristics of many teeth, the diastema, **\*822** or spacing between the teeth, as well as “drag marks” where the tissue slid between the biter's jaws.

Karazulas then compared the models made of the defendant's teeth with the various photographs of the bite mark. He testified that any unique or identifiable characteristics of the defendant's dentition depicted in the models appeared to have a corresponding mark on the victim's breast, and likewise, that the markings on the breast of the victim contained a corresponding mark for every unique characteristic of the defendant's dentition.

Lastly, Karazulas engaged in a series of steps that eventually led to the creation of the Adobe Photoshop overlays at issue in this case. First, he made a wax impression using the plaster molds taken of the defendant's teeth. <sup>FN35</sup> Karazulas then placed the upper and lower molds of the defendant's teeth onto a copy machine and printed out an image from these molds. Next, placing paper over that image, and holding it over a lighted surface, he manually **\*\*948** traced out the biting edges of the teeth. That tracing was then photocopied <sup>FN36</sup> onto a clear piece of acetate, producing a transparent overlay depicting the edges of the

defendant's dentition.<sup>FN37</sup>

FN35. Karazulas testified that this wax impression revealed the shape of the jaw and the arch of the teeth, the diastema, as well as the depth into the wax that each tooth entered, which in turn illustrated the varying length and width of each tooth. The impression also revealed the cutting edges of the teeth, that some teeth were tipped forward more than others and that some teeth were further back in the mouth than others.

FN36. The record reveals that some of the dentition tracings were created with the use of a computer scanner, instead of a photocopier.

FN37. Karazulas testified that the acetate tracings demonstrated several unique characteristics of the defendant's dentition, including two rotated cuspids, two incisors that were tipped forward, and diastema between numerous teeth.

Karazulas then had both enhanced and unenhanced photographs of the bite mark, as well as tracings of the \*823 defendant's dentition, scanned into a computer. Because he was not familiar with Adobe Photoshop, and was using the program for the first time for an odontological match, Karazulas secured the assistance of Gary Weddle, a Fairfield University chemistry professor, to scan these images and create the overlays by using the computer program to superimpose the defendant's dentition over the bite mark.<sup>FN38</sup> Karazulas relied on Weddle because he lacked the ability to do the superimpositions himself. Over the course of two days, Karazulas spent approximately seven to eight hours watching Weddle create the overlays. Karazulas testified that he instructed Weddle not to alter the original images in creating the overlays.

FN38. The record does not reflect why Weddle did not testify at trial.

Using the Adobe Photoshop program, Karazulas testified that Weddle created a number of overlays. These overlays can be categorized into two types. First, there are overlays, such as state's exhibits 117 and 166, that are composed of tracings of the defendant's dentition superimposed over cropped photographs of the bite mark, both enhanced and unenhanced. Second, there are overlays composed of images of the defendant's actual teeth superimposed over photographs of the bite mark. This type of overlay, as depicted in state's exhibits 118 through 121, as well as state's exhibit 164, was created by: scanning portions of the molds taken of the defendant's teeth to create state's exhibit 115;<sup>FN39</sup> directing the computer software to isolate the upper layers of the occlusal edges of the molds from the images contained in state's exhibit 115; applying a process to the images of the teeth whereby the teeth became less \*824 opaque and more transparent; and lastly, superimposing the image of the translucent teeth over various photographs of the bite mark. On the basis of these processes, Karazulas concluded that the defendant had bitten the victim's breasts.

FN39. Karazulas described the creation of state's exhibit 115 as follows: "[The] models [of the defendant's teeth] are laid on a scanner, [on] top of the glass. The scanner top is closed. And you go through a process of scanning with the Adobe Photoshop program. And the image from the scanner goes into the computer. And after this image appears on your screen, you press print and this comes through the printer."

Referring to state's exhibit 119, an Adobe Photoshop overlay composed of an image of the defendant's translucent upper teeth superimposed over an

unenhanced photograph of the bite mark, Karazulas testified as follows: “I observed that the shape of the bite mark on the breast and the arch that the teeth edges made were very consistent. And very pointedly the left central incisor, the tipping forward matched the discoloration of the bite mark area on the breast, and there is a noticeable gap without a mark where the cuspid on the upper left side is rotated. And the marks above the teeth to the left are pretty consistent with the shape of those incisal edges.” Commenting on state's exhibit \*\*949 117, an Adobe Photoshop overlay composed of tracings of the defendant's upper dentition superimposed over an unenhanced photograph of the bite mark, Karazulas testified: “It gives me the shape of the arch. A match of the arch is consistent with the mark above it. The upper front central incisor, left one, protrudes beyond the line or curvature matching the markings in the bite mark. And there are other marks of each of these two above that correspond to the circumference.” Karazulas also testified with regard to state's exhibit 120, an Adobe Photoshop overlay composed of an image of the defendant's translucent upper teeth superimposed over a Lucis-enhanced photograph of the bite mark, stating: “We can see where each individual tooth falls into line with the discolorations on the breast and all the particular nuances, the upper left central incisor and the lateral, the arch bulges out. And the corresponding marks of the other teeth seem to fall right into the arch very well.” He also stated, noting state's exhibit 121: “There's \*825 a very good relationship between the marks on the breast and each of the individual teeth in the lower jaw. Each tooth seems to fit into the pattern very well.”

The defendant objected to the admission of these overlays for lack of foundation.<sup>FN40</sup> The state argued that a proper foundation had been laid because Karazulas could testify that the scanned photographs appearing in the overlays were fair and accurate renditions of the original photographs of the bite mark, and that the scanned tracings or scanned dental molds appearing in the overlays were fair and accurate ren-

ditions of original acetate tracings or original dental molds of the defendant's dentition and, therefore, through authentication of the component parts, or individual layers, of the exhibits, the overlays themselves were authenticated. In essence, the state argued that Karazulas' lack of knowledge about *how* the computer generated the evidence was irrelevant, reasoning that, because two pieces of reliable evidence had gone into the computer, what came out of the computer therefore necessarily had to be reliable.

FN40. We note that the defendant's objection extended to both types of overlays—those that used dentition tracings and those that used scans of the dental molds.

The defendant argued that the reliability of what had come out of the computer was the issue, and that he could not test that reliability by questioning a person who merely had sat next to the machine. The defendant referred to the issue at hand as a “black-box phenomenon,” whereby the jury was being asked to trust the computer. The defendant further argued that, although two separate images that could be authenticated were “fed” into a computer, there was no way for Karazulas to authenticate independently the result of the two images being superimposed other than by saying that the resulting product was a fair and accurate representation \*826 of what “came out” of the computer. The defendant pointed out that the reliability of what had gone into the computer does not ensure that the evidence coming out of the computer is also reliable, and that a witness who had spent almost eight hours merely watching another person create the superimposition was “uniquely disqualified” to testify regarding the inner machinations of the computer that had produced the evidence. The defendant argued that it was impossible for him to test the reliability of the machine itself or the process used with a witness who could attest, based on the naked eye, only to the fact that the exhibit produced at trial was a fair and accurate representation of what came out of the machine. As the defendant pointed out: “[T]here were two steps.

There was a scan. There was transmission of one form of data into another form. \*\*950 There are questions about the accuracy of the transmission. Then that went in somewhere and was translated into ... the digital impulses that are computers. Then they were sorted by some process and they were superimposed one upon the other. It's not enough to say ... A looks like A, B looks like B, and look what the computer did."

The trial court admitted the Adobe Photoshop images. The court reasoned that Karazulas' expertise was the important factor in determining whether the images should be introduced into evidence because it was his expertise that could judge whether the finished product accurately represented subjects or items or the juxtaposition of subjects and items about which he is an expert, not the computer expert who may have facilitated the creation of the exhibits.

On appeal, the state resurrects its argument that, because the exhibits used to create the overlay—the photographs of the bite mark and the tracings or molds of the defendant's teeth—were authenticated properly, the overlay itself, as a product of the two, was authenticated\*827 as well.<sup>FN41</sup> In addition, the state claims that the overlays created by Adobe Photoshop are the equivalent of what could be seen if a tracing of the defendant's teeth manually were placed over a photograph of the bite mark.

FN41. Additionally, the state argues on appeal that the overlays, like the enhanced photographs, constituted mere "illustrative" evidence. We disagree with this contention. See footnote 20 of this opinion. Likewise, we are not persuaded by case law cited by the state in support of admissibility of evidence created by Adobe Photoshop wherein the question before that court involved a challenge concerning a poster created by Adobe Photoshop that had *not* been admitted as substantive evidence. See *State v. Bauer*, 598 N.W.2d 352, 362–63 (Minn.1999)

("[b]ecause the trial court did not receive the poster as substantive evidence ... we need not decide whether the proper foundation was laid").

[19][20] The defendant claims on appeal that, "[i]n this case, the computer was used to *create* a picture which did not exist before," and that "[a] dramatic new technique was used to *create* the single most important piece of evidence offered...." (Emphasis in original.). Unfortunately, we find ourselves incapable of evaluating just how true these assertions are and that inability underscores the problem at issue here.<sup>FN42</sup> Unlike Palmbach's ability to testify regarding the Lucis enhancement process, Karazulas was not able to testify in accordance with the standard set forth in part I A of this opinion; specifically, he could not testify as to whether the computer processes that were used to create the overlays were accepted in the field of odontology as standard and competent,<sup>FN43</sup> whether proper procedures were followed\*828 in connection with the input and output of information,<sup>FN44</sup> whether Adobe Photoshop was reliable for this sort of \*\*951 forensic application,<sup>FN45</sup> or whether the equipment was programmed and operated correctly. Nor was Karazulas capable of testifying that a qualified computer operator was employed; he could testify only that, because he did not know enough to perform the process himself, he had someone else do it. In fact, when asked how the computer actually superimposed the tracing of the biting edges of the defendant's teeth over the photograph, Karazulas merely stated that "Weddle ... moved them together." Moreover, we note that Palmbach testified that, unlike the Lucis program, the Adobe Photoshop program was capable of actually altering photographs.<sup>FN46</sup>

FN42. Just as the enhanced photographs did not fall cleanly into one of two "types" of computer generated evidence, either animation or simulation; see part I A of this opinion; these overlays of the defendant's dentition over images of the bite mark are not

exactly animations, but they are nearly so. Therefore, they, too, will be considered computer generated evidence for the purposes of this opinion.

FN43. We note that the state attempted to have Palmbach testify as to the program's acceptance in the field. Palmbach stated: "I am aware of applications, and I'm also personally aware of uses within the odontology field. I've read several papers in which they've spoken of the use of programs, specifically Adobe Photoshop, to use in their bite mark analysis." This testimony, however, does not establish adequately that the program has been proven reliable enough to be deemed "competent" or that it has become standard practice in the field.

FN44. In fact, the defendant claims that Karazulas deviated from proper procedure in producing the Adobe Photoshop overlays.

FN45. The state points out that the defendant's own expert testified that, according to the American Board of Forensic Odontology, Adobe Photoshop is an appropriate aid in bite mark identification. This, however, does not conclude our inquiry in this matter, because identifying a tool or process as an "aid" does not satisfy our multifaceted standard.

FN46. Palmbach testified: "Now, [Adobe] Photoshop has ... a lot of features, many of which I'll be the first to say I don't know or use. But some of those features will allow you to filter out components, some of them will allow you to cut and crop and paste components." Palmbach further testified that Adobe Photoshop "certainly has features where you can take multiple images and bring them in and out of plane in an attempt

to overlay them over each other or rotate them and try to align them. So it has that moving, cropping, editing, [and] overlaying capability."

Karazulas, a highly qualified odontologist, recognized his own limitations as a witness with respect to the Adobe Photoshop evidence. He admitted that he had "no skill or experience" with Adobe Photoshop. When asked whether the computer bent the image in some respects in order to account for the curvature of a three-dimensional object, such as a breast, when the computer is actually superimposing one two-dimensional\*829 flat image onto another, Karazulas responded that he did not think that the computer could do so, but stated: "I'm not an expert in it, but I think we [can] get somebody who knows computers, they can explain that."

Karazulas also testified that the images of the defendant's teeth, which had been produced by scanning the molds of his teeth, had also been subjected to a process whereby Adobe Photoshop "cut layers" in order to make the images of the teeth less opaque for purposes of the superimposition. This "layering" effect allows the program user to adjust the opacity of an object in order to see other images *through* the object—in other words, to make one object nearly transparent. When asked about Adobe Photoshop's capability to create this see-through effect, Karazulas had trouble describing it. "We'd have to ask an Adobe [Photoshop] expert, I guess, or a technician what that means, but when you see it done on the screen, it makes sense." Later, in response to direct questioning from the trial court concerning this same process, Karazulas stated: "Judge, you got me," "I don't know how they do it, but they do it," and "I think we really need an engineer."

[21] A witness must be able to testify, adequately and truthfully, as to exactly what the jury is looking at, and the defendant has a right to cross-examine the witness concerning the evidence.<sup>FN47</sup> Without a \*\*952

witness who satisfactorily<sup>\*830</sup> can explain or analyze the data and the program, the effectiveness of cross-examination can be seriously undermined, particularly in light of the extent to which the evidence in the present case had been “created.” Karazulas lacked the computer expertise to provide the defendant with this opportunity.<sup>FN48</sup> For example, in response to a question asked by defense counsel regarding the superimposition of the image of the defendant's teeth over the bite mark, Karazulas responded: “I see [Weddle] do it with the mouse and I see him clicking things; but, I mean, you have to be very experienced.” Later in the cross-examination, Karazulas explained the software this way: “Adobe [Photoshop] can put a picture on your screen, and then you could take a model and scan that into the photograph and you can make matches.” In particular, Karazulas also could not articulate sufficiently how the visual effect of the defendant's translucent teeth superimposed over the bite mark was produced.<sup>FN49</sup> The defendant should have had the opportunity to question someone who could testify accurately as to the reliability of the evidence and the processes used to generate it. In this <sup>\*831</sup> case, one possible candidate was the person who “created” the overlay—Weddle, the Fairfield University professor whom Karazulas had used to craft the superimposition of the defendant's dentition over the images of the bite mark.<sup>FN50</sup> We conclude that, based on the standards discussed in part I A of this opinion, the trial court improperly admitted the Adobe Photoshop overlays.<sup>FN51</sup>

FN47. We recognize that Karazulas testified that, to the naked eye, the portion of the bite mark photographs, the manual and computer copies of the tracings of the defendant's dentition, and the scanned images made from the molds of the defendant's teeth that appeared in the computer generated overlays were all fair and accurate portrayals of their original corresponding evidence, which had been marked as exhibits at trial. Because odontological matching depends on millimeters, a

millimeter or two either way could make the difference between a point of concordance and a point of discordance. A visual inspection of the separate pieces, therefore, was not enough to ensure the reliability of the superimpositions.

Karazulas further testified that there had been no alteration between the scanned images and the images that appeared in the superimpositions. Although he testified that he “asked [Weddle] not to make any changes” to the images of the original exhibits when creating the overlays, Weddle himself did not testify that he had not, in fact, made any changes, nor was Karazulas proficient enough in the process used to create the overlays to determine for himself whether, in fact, Weddle had altered or manipulated the exhibits in the process of using the Adobe Photoshop software.

FN48. The state also had Palmbach testify briefly regarding Adobe Photoshop, but his testimony regarding the program fails to illuminate the subject. He testified merely that he was “generally” familiar with the Adobe Photoshop program and its uses in forensic science, but admitted that there were many features that he did not understand or use.

FN49. Karazulas testified: “I guess it works like an MRI [magnetic resonance imaging], and you can select the layers as you cut through an object. So as ... Weddle went through the process, I would say, ‘Hold it. That's it. That's what we need.’ We needed the teeth. Because they have a thing called the opaquer or the opacity maker. And as you change the dial, then you would see through the object a little more clearly. So we did this for two or three hours until we got what we thought was the incisal edges and enough

opacity to move these edges to the marks.”

FN50. Weddle, by nature of his role in the actual creation of the overlays, is the most obvious choice to be the person qualified to testify regarding the Adobe Photoshop program, but we make no determination regarding whether his testimony, in and of itself, would have been enough to establish the reliability of this evidence.

FN51. Once courts are satisfied with the inherent reliability of computer programs, like Lucis and Adobe Photoshop, we note that a trial court may dispense with imposing on the offering party the burden of meeting more stringent foundational requirements. Compare *Dyson v. New York & New England R.R. Co.*, supra, 57 Conn. at 24, 17 A. 137 (offer of photographs accompanied by testimony of photographer who took them as to their accuracy, and of surveyor who identified points of view) with *McGar v. Bristol*, supra, 71 Conn. at 655, 42 A. 1000 (photographer's in-court testimony not essential). Furthermore, we recognize that “[t]he potentially limitless application of computer technology to evidentiary questions will continually require legal adaptation.” *Penny v. Commonwealth*, 6 Va.App. 494, 499, 370 S.E.2d 314 (1988) (concluding that Virginia courts may admit telephone “call trap” results into evidence only after reliability of particular trap has been shown). Until the reliability of computer programs are no longer questioned, however, we rely on the factors enunciated in this opinion to guide the admissibility of such evidence.

**\*\*953** [22][23][24] In light of this conclusion, we next must consider whether the admission of the Adobe Photoshop overlays violated the defendant's constitutional rights, or whether the error was merely

evidentiary in nature. See *State v. Morales*, 78 Conn.App. 25, 38, 826 A.2d 217 (“[w]e begin our analysis by considering whether the defendant has actually raised a claim of constitutional magnitude or whether he is robing a garden variety evidentiary claim in the majestic garb of constitutional claims”), cert. denied, 266 Conn. 901, 832 A.2d 67 (2003). The defendant claims that the admission of this evidence without a proper foundation obstructed his constitutional\*832 right to confrontation. “The right to confrontation is fundamental to a fair trial under both the federal and state constitutions. *Pointer v. Texas*, [supra, 380 U.S. at 403, 85 S.Ct. 1065]; *State v. Jarzbek*, 204 Conn. 683, 707, 529 A.2d 1245 (1987), [cert. denied, 484 U.S. 1061, 108 S.Ct. 1017, 98 L.Ed.2d 982 (1988)].... It is expressly protected by the sixth and fourteenth amendments to the United States constitution; <sup>FN52</sup> *Davis v. Alaska*, [supra, 415 U.S. at 315, 94 S.Ct. 1105]; *Pointer v. Texas*, supra at [403, 85 S.Ct. 1065]; and by article first, § 8, of the Connecticut constitution. *State v. Torello*, 103 Conn. 511, 513, 131 A. 429 (1925).” (Citation omitted.) *State v. Hufford*, 205 Conn. 386, 400–401, 533 A.2d 866 (1987).

FN52. “The confrontation clause of the sixth amendment is made applicable to the states through the due process clause of the fourteenth amendment.” *State v. Sandoval*, 263 Conn. 524, 532 n. 17, 821 A.2d 247 (2003).

[25][26][27][28][29] “Our analysis of the defendant's claim is guided by the familiar constitutional guidelines relevant to cross-examination by the defendant in a criminal trial. It is axiomatic that the defendant is entitled fairly and fully to confront and to cross-examine the witnesses against him.” (Internal quotation marks omitted.) *State v. Reynolds*, 264 Conn. 1, 58, 824 A.2d 611 (2003). “The confrontation clause ... requires that the defendant be accorded some irreducible minimum of cross-examination into matters affecting the reliability and credibility of the state's witnesses.” *State v. Ortiz*, 198 Conn. 220, 224, 502 A.2d 400 (1985). “The defendant's right to

cross-examine a witness, however, is not absolute.” (Internal quotation marks omitted.) *State v. Francis*, 267 Conn. 162, 181, 836 A.2d 1191 (2003). “We have observed that a defendant’s right [to cross-examination] is not infringed if the defendant fails to pursue a line of inquiry open to him.... The test is whether the opportunity to cross-examine existed, not whether full use of such opportunity was made.” (Internal quotation marks omitted.) \*833 *State v. Delgado*, 261 Conn. 708, 720, 805 A.2d 705 (2002). “In order to comport with the constitutional standards embodied in the confrontation clause, the trial court must allow a defendant to expose to the jury facts from which the jurors, as the sole triers of fact and credibility, could appropriately draw inferences relating to the reliability of the witness.... In determining whether a defendant’s right of cross-examination has been unduly restricted, we consider the nature of the excluded inquiry, whether the field of inquiry was adequately covered by other questions that were allowed, and the overall quality of the cross-examination viewed in relation to the issues actually litigated at trial.” (Internal quotation marks omitted.) *State v. Sandoval*, 263 Conn. 524, 535, 821 A.2d 247 (2003).

**\*\*954** [30] We recognize that foundational questions are generally of an evidentiary nature, and, in most instances, a mere evidentiary error will not rise to the level of a constitutional error. *State v. Vitale*, 197 Conn. 396, 403, 497 A.2d 956 (1985) (“[e]very evidentiary ruling which denies a defendant a line of inquiry to which he thinks he is entitled is not constitutional error”). The present case, however, is somewhat unique, based on the nature of the evidence, its significance to the case and the witness’ inability to attest to its trustworthiness. We therefore inquire whether the court’s ruling that the evidence had a satisfactory foundation, and the subsequent omission of testimony from Weddle, or any other person knowledgeable about the processes that created the evidence in this case, infringed on the defendant’s right to confrontation.

The relevant scope of inquiry in the present case is whether the defendant was given an adequate opportunity to cross-examine Karazulas concerning his identification of the defendant as the biter. To that end, we observe that Karazulas’ conclusion that the defendant’s dentition matched the bite mark on the victim’s breast involved several admissible building blocks, including \*834 molds of the defendant’s teeth, a wax impression taken from the molds, acetate tracings of the biting edges of the defendant’s teeth, and enhanced and unenhanced photographs of the bite mark. The defendant had the opportunity to cross-examine Karazulas freely regarding all of these exhibits and how they informed his conclusion. Any failure to take full advantage of such an opportunity does not render the improper admission of the Adobe Photoshop overlays, just one part of the evidentiary whole, a confrontation issue.

Moreover, we note that the defendant had his own expert use the Adobe Photoshop overlays to support his conclusion that the defendant was not the biter. Neal Riesner, a forensic dentist, testified on behalf of the defendant that, to a reasonable medical certainty, the state’s exhibits, including the overlays, did not reflect a match between the defendant’s dentition and the bite mark. For example, regarding state’s exhibit 121, an Adobe Photoshop overlay of an image of the defendant’s translucent lower teeth over a Lucis enhanced photograph of the bite mark, Riesner specifically pointed out that there was a tooth with no corresponding mark and that the overlay revealed no individual characteristics of the teeth. Riesner testified that state’s exhibit 119, an Adobe Photoshop overlay composed of an image of the defendant’s translucent upper teeth superimposed over an unenhanced photograph of the bite mark, and state’s exhibit 117, an Adobe Photoshop overlay composed of tracings of the defendant’s upper dentition superimposed over an unenhanced photograph of the bite mark, depict the bite mark as having a wider arch than the defendant’s teeth. According to Riesner, state’s exhibit 118, an Adobe Photoshop overlay of an image of the de-

fendant's translucent lower teeth over an unenhanced photograph of the bite mark, revealed a tooth that was wider than its corresponding mark, teeth with no corresponding \*835 marking, and a crack between two teeth with no corresponding mark. Additionally, state's exhibit 120, an Adobe Photoshop overlay composed of an image of the defendant's translucent upper teeth over a Lucis enhanced photograph of the bite mark, revealed a rotated maxillary right cuspid with no corresponding mark. Riesner testified that there were no visible concordant points between the defendant's dentition and the bite mark that were visible from viewing state's exhibits 117, 118, 119 or 121.

In addition to pointing out defects in the component exhibits Karazulas used to create the overlays, Riesner complained about \*\*955 the quality of the Adobe Photoshop overlays themselves. He insisted that the images were too cloudy or blurry to allow a positive match. He also testified that the computer generated overlays were problematic because they entailed the "arbitrary select[ion]" of "levels" of the images, thus falsely increasing the appearance of a match between the defendant's dentition and the bite mark. <sup>FN53</sup> He also pointed out that the computer generated overlays relied on flattened images of a curved surface. In addition, Riesner stated that he could not tell if anything in the images that appeared in the overlay had been "corrected." He disagreed that computer generated overlays were the "gold standard" compared to other methods of generating overlays, and further disagreed that computer generated overlays provided "the most reproducible and accurate exemplars."

FN53. Referring to state's exhibit 120, Riesner testified: "[N]ow, let's remember this is a trick of the computer. You're looking ... from the root side of the teeth. You're not looking down on it. So this is a computer generated thing. I mean, you've got something here that's a layer so you're looking at

it. What you're looking at is this. What you see is this tooth that's turned here is this tooth on this side and you're looking down on it because it's creating it this way. So you can't look at it this way and make a judgment. (Indicating.)"

\*836 Riesner's ability to testify from the Adobe Photoshop overlays that there was no match between the defendant's dentition and the bite mark, even considering his criticism of the overlays, undermines the significance of the defendant's inability to question Weddle, or anyone else, regarding how those exhibits were actually created. As Riesner's testimony makes clear, the defendant was given an opportunity to reveal adequately the infirmities of Karazulas' conclusion. Riesner's testimony actually highlighted the potential lack of reliability of the evidence for the jury, and so, his ability to testify from the overlays closed any gaps concerning those things on which the defendant was unable to cross-examine Karazulas directly.

Therefore, we determine that the trial court's ruling did not, under all of the circumstances in this particular case, have the effect of violating the defendant's right of confrontation. See *State v. George*, 194 Conn. 361, 366, 481 A.2d 1068 (1984) (trial court's "isolated ruling does not in the context of the whole case amount to a deprivation of the opportunity to reveal the facts from which the jury could appropriately draw inferences relating to the reliability of the witness" [internal quotation marks omitted] ), cert. denied, 469 U.S. 1191, 105 S.Ct. 963, 83 L.Ed.2d 968 (1985). In satisfaction of his right to confrontation, the defendant had a meaningful opportunity to probe the reliability of Karazulas' identification testimony. Thus, the error was evidentiary in nature and not constitutional.

[31][32] Accordingly, we shall examine whether the evidentiary impropriety was harmless. In order to establish reversible error on an evidentiary impropriety, the defendant must "demonstrate that it is more

probable than not that the erroneous action of the court affected the result.... \*837 *State v. Meehan*, 260 Conn. 372, 397, 796 A.2d 1191 (2002).” (Internal quotation marks omitted.) *State v. Kirsch*, supra, 263 Conn. at 412, 820 A.2d 236.<sup>FN54</sup>

FN54. “In *State v. Meehan*, supra, 260 Conn. at 397 n. 13, 796 A.2d 1191, we reiterated that two lines of cases had developed in addressing the standard for reversing nonconstitutional evidentiary improprieties: One line of cases states that the defendant must establish that it is more probable than not that the erroneous action of the court affected the result.... A second line of cases indicates that the defendant must show that the prejudice resulting from the impropriety was so substantial as to undermine confidence in the fairness of the verdict.” (Internal quotation marks omitted.) *State v. Kirsch*, supra, 263 Conn. at 412 n. 16, 820 A.2d 236. As in *Kirsch*, we conclude that the defendant in the present case has failed to prove the requisite harm under either standard. *Id.*

**\*\*956** The defendant claims that the admission of the computer generated evidence was harmful in light of Karazulas' reliance on the improperly admitted exhibits, as well as the absence of other compelling evidence connecting him to the crime. Specifically, the defendant points to the fact that the bite mark match critically depended on the Adobe Photoshop software. First, the defendant argues that, solely on the basis of the molds and tracings of the defendant's teeth and the photographs of the bite mark, Karazulas testified generally about a few characteristics common to both. On the basis of his review of all the exhibits, specifically the Adobe Photoshop overlays, however, Karazulas testified regarding fifteen unique characteristics. Second, the defendant refers us to several points in Karazulas' testimony demonstrating his reliance on the Adobe Photoshop overlays to conclude that the defendant was the biter. In sum, the defendant

asserts that, when testifying to the match visible in the Adobe Photoshop exhibits, Karazulas described the bite marks as being “very consistent” and having a “very good relationship” with the defendant's dentition. In contrast, regarding the original match made before the use of the Adobe Photoshop software, Karazulas stated that he “saw a match there from the old technique we used.” The defendant also refers us to several places in the transcript wherein \*838 Karazulas describes the impact of the Adobe Photoshop software on his ability to be confident in the match as proof that the inadmissible overlays were an indispensable part of Karazulas' conclusion. Therefore, in light of the perceived objectivity of the evidence because it was computer generated, and the strong visual impact that such evidence could have had on the jury, the defendant claims that the harm suffered was overwhelming.

In addition, the defendant points out that the harm from the overlays is not eliminated merely because the jury could have compared them with properly admitted exhibits, because jurors are not qualified to engage in odontological matching. More important, the defendant argues, because an odontological match requires pinpoint accuracy, visual inspection by laypersons is not an adequate substitute for testimony establishing the accuracy of an exhibit. The defendant also contends that jurors tend to give considerable weight to “scientific” evidence, and that the possibilities that a “juror would ignore the opinion of an expert based upon the juror's own visual inspection are quite remote.” Specifically, after Karazulas' testimony characterizing the computer match as “scientific” and incapable of error, and after the exhibits were admitted into evidence, according to the defendant there was no reason for the jury to “recreate” the overlays themselves in order to examine them and determine the extent to which they matched their corresponding individual parts.

Lastly, the defendant claims that the bite marks were the only physical evidence connecting him to the

victim. Without the match of his teeth to the bite mark, the defendant argues, the state's case consisted of nothing more than a nondescript bra, common household objects—safety pins and garbage bags—and admissions made by the defendant to individuals involved with \*839 drugs and crime. The defendant contends that no jury would have convicted him on such “flimsy” evidence.<sup>FN55</sup>

FN55. The defendant also maintains that the state's treatment of the issue of harmlessness constitutes inadequate briefing because it addressed the issue in a series of cursory footnotes. See *State v. Ruscoe*, 212 Conn. 223, 241 n. 9, 248, 563 A.2d 267 (1989), cert. denied, 493 U.S. 1084, 110 S.Ct. 1144, 107 L.Ed.2d 1049 (1990). Although we agree that the state's handling of the issue was deficient, our determination that the evidence was improperly admitted nevertheless necessitates that we address the harm.

**\*\*957** In response, the state first relies on its incorrect assertion that, because the overlays only served to “illustrate” Karazulas' conclusion; see footnotes 20 and 41 of this opinion; instead of serving as actual evidence that resulted in identification of the defendant as the biter, the admission of the overlays was harmless. Second, the state asserts that any harm caused by the overlay was ameliorated by the jury's ability to test the accuracy of what the computer had generated by taking the original exhibits and manually laying one over the other to see if it could replicate the computer's results.<sup>FN56</sup> Finally, the state relies on the other evidence produced at trial to prove harmlessness. Specifically, the state points to the existence of the victim's bra and the brown trash bags, discovered in and around the defendant's \*840 apartment building, the safety pins found in the defendant's van, and the various confessions and incriminating statements the defendant made to Arnold, Scalise, and others. After a careful review of the record, we agree with the state that the evidence produced at trial mitigates any

harm that resulted from the improper admission of the overlays.

FN56. The state argues that the admission of the Adobe Photoshop overlays constituted harmless error because the jury was able to test the accuracy of what the computer had generated by taking the original exhibits and manually laying one over the other to replicate the computer's results. This is true, however, only for those few exhibits composed of tracings of the defendant's dentition superimposed over photographs of the bite mark. It would be impossible for anyone to recreate, manually, those overlays depicting translucent images of the defendant's teeth superimposed over the bite mark.

We note that Karazulas did reconstruct the “overlay” technique manually for the jury. Karazulas testified that, by taking an acetate tracing of the defendant's teeth and placing it over a photograph of the bite mark, it gave him “an idea of the general edges and the shape of the bite mark [in] relation to the model.” Karazulas additionally testified that, by sliding an acetate tracing of the defendant's teeth over an enhanced photograph of the bite mark, he observed that “[the] pattern generated by the teeth was compatible with the pattern on the breast.”

Karazulas' conclusion, following his examination of the overlays, that the defendant was the biter was definitive and to the highest degree of certainty. Karazulas stated: “I believe that with reasonable medical certainty without any reservation that these marks were created by [the defendant's] teeth.” Importantly, however, Karazulas testified that he also had rendered an opinion in this case in 1998, prior to the use of the Lucis and Adobe Photoshop software programs, and that his opinion in 1998 also involved a

conclusion “to a reasonable degree of medical certainty,” the highest certainty in the field. We note that Karazulas testified that, throughout his career, he had examined approximately 5000 different bite marks. In addition, he testified that there were numerous situations in which he was asked to render an opinion as to bite mark evidence, but that, unlike the present case, he frequently determined that such evidence was inadequate from which to draw a conclusion. This testimony informs the level of certainty he displayed regarding his pre-Adobe Photoshop identification of the biter. Therefore, although it may be true that, as the defendant contends, the majority of Karazulas’ testimony regarding his conclusion that the defendant was the biter centered around the match that was visible from the Adobe Photoshop exhibits, that does not mean that Karazulas relied on those exhibits, before trial, to establish **\*958** such a match. In fact, the testimony reveals otherwise. When asked whether he was “just as certain prior to the use of the computer,” Karazulas answered in the affirmative, but subsequently added **\*841** that “if anything, [his conclusion had] gotten stronger” due to the availability of Adobe Photoshop.

As we previously have discussed, Karazulas testified that the molds of the defendant’s dentition demonstrated several unique characteristics, including two rotated cuspids, two tipped incisors and a slanted arch. A wax impression taken from the molds revealed some of the same characteristics, as well as diastema, and the uneven length of some of the defendant’s teeth. Karazulas further testified that acetate tracings also illustrated these unique characteristics. In addition, Karazulas was able to compare all of these exhibits, which represented the defendant’s dentition, with photographs of the bite mark. Karazulas testified that the quality of the bite mark was “excellent,” and that from it he could “see the circumference of the arch and ... [the] individual characteristics of many teeth.”

Notably, at one point in the testimony, in an attempt to recreate the experiments that Karazulas em-

ployed to establish the time of the bite in relation to the victim’s death, defense counsel used the molds of the defendant’s teeth to put a “bite mark” on his own arm. Karazulas used this opportunity to point out to the jury the unique marks the molds left on defense counsel’s skin. Addressing the jury, Karazulas stated: “I’m going to show them what a diastema looks like. Now, look. See that space? That’s because the cuspid is turned. Now, look at this left cuspid sticking up. Exactly like the photograph. You did wonderful. Let’s show the rest of the jury. Because that cuspid is turned, the point is in a different place, there’s a diastema. There’s the central. And it’s above this central. These two come up. Beautiful. Show these people. The photograph in my eyes looks just like what we have here. There’s the diastema because of the rotated cuspid. Here’s the central incisor above the plane of the lateral. Here’s the diastema on the other side.” It is clear, then, from our review of **\*842** the record, that Karazulas’ ultimate conclusion that the defendant was the biter did not rely upon the Adobe Photoshop overlays, but instead depended on Karazulas’ studied comparison of properly admitted exhibits, such as the molds of the defendant’s teeth, a wax impression taken from the molds, tracings of the defendant’s dentition, and the enhanced and unenhanced photographs of the bite mark, as well as a persuasive impromptu demonstration in front of the jury. The Adobe Photoshop overlays served merely to augment the certainty of his conclusion.

We conclude that Karazulas’ properly admitted testimony regarding exhibits other than those created using Adobe Photoshop goes a long way in rendering harmless the improperly admitted evidence. In the next stage of this inquiry, we turn to the other evidence that was before the jury. The physical evidence in this case included a black bra, identified as the one the victim wore on the night of her murder, and trash bags, like the one wrapped around the victim’s body, found in and around the defendant’s apartment building in Stafford Springs, as well as safety pins found in his van. In addition to these items, there was considerable testimony regarding the numerous confessions and

other incriminating statements the defendant had made to several different witnesses, including a police lieutenant, a journalist, a shop manager, a coworker and his landlord.

Specifically, the defendant revealed his anger toward women and prostitutes to \*\*959 many different witnesses, stating that women like the victim “get what they deserve.” The defendant also made incriminating remarks during an interview with a journalist. In response to being asked why the killer could not stop murdering women, he stated, “If I knew that, I would stop tomorrow.... So somebody could live.” Moreover, the defendant told several acquaintances that he \*843 had “gotten away” with murder. When his landlord asked the defendant what it was like to rape and kill a woman, he grinned and laughed aloud. When one of the defendant's coworkers asked him what it felt like to strangle a woman, the defendant responded by violently choking the man. Lastly, Scalise, a fellow inmate at the time of the defendant's trial, testified to numerous conversations in which the defendant offered detailed accounts of the victim's murder. The defendant confessed to Scalise that he had bitten the victim on the breast while having sex with her, had beaten her in the face, and had strangled her. He admitted to Scalise how, after he had killed the victim, he had taken her bra and underwear, “bagged” her, and then “dumped” her body in a snow bank near a university. The defendant admitted to removing the safety pin from the victim's bra and later using it to repair his van. There is no indication in the record that Scalise became aware of such accurate details of the crime from any source but the defendant.

The defendant argues that most of the witness' testimony against him was impugnable. Specifically, he draws our attention to the fact that Arnold, Mills and Stallings were all addicted to and under the influence of drugs at various times before, during and after the defendant made statements to them. In addition, the defendant points out that both Arnold and Scalise were incarcerated at the time they shared with

the police information concerning the defendant, and suggests that their incarceration gave them a motive to cooperate with the state. Lastly, the defendant asserts that some of the witnesses had personal reasons for testifying against him. Specifically, Mills admitted that she testified, in part, because her sister was the victim of a homicide, and Arnold testified that he had strong “personal feelings” for the victim. Regardless of these possible infirmities, however, the jury *could* have credited \*844 the testimony of these witnesses and we continually have held to the rule that we will not judge the credibility of witnesses nor substitute our judgment for that of the trier of fact. See *PSE Consulting, Inc. v. Frank Mercede & Sons, Inc.*, 267 Conn. 279, 312, 838 A.2d 135 (2004) (“[i]ssues of credibility are uniquely within the province of the jury”); *State v. Francis*, supra, 267 Conn. at 187, 836 A.2d 1191 (jailhouse witnesses no less reliable than other witnesses).

Therefore, in light of the numerous confessions and other incriminating statements the defendant made to several people, as well as the aforementioned physical evidence, in combination with Karazulas' testimony regarding properly admitted exhibits that tied the defendant inextricably to the bite mark, we conclude that the improper admission of the Adobe Photoshop overlays was harmless.

## II

[33] We next turn to the defendant's claim that the trial court improperly declined to mark as an exhibit certain documents that were not offered into evidence. Specifically, Rovella, the lead investigator in this case, referred to some of his numerous police reports dating back to 1991 in order to refresh his recollection during direct examination. No attempt was made to have those items marked for identification nor was there any objection to their use. During cross-examination, the defendant asked Rovella whether earlier, during \*\*960 his direct examination, he had refreshed his memory by referring to documents that were inside an “envelope.” Rovella acknowledged that he had. Rov-

ella also acknowledged that the envelope contained other documents that he had not relied on. The defendant then asked to have all of the documents inside the envelope marked for identification. The state objected and the court ruled that the defendant could examine only those documents \*845 that Rovella had used to refresh his recollection. The defendant then asked Rovella to remove from the envelope those documents that he had used to refresh his memory. In an effort to comply, Rovella removed from the envelope all of the documents that he had authored. Although Rovella was able to identify one document that he had used to refresh his memory, he was not able to identify a second document that he had used.

On appeal, the defendant claims that the trial court improperly denied his request to mark for identification Rovella's envelope and everything contained therein. Specifically, he contends that the trial court's failure to mark those items deprived him of the opportunity to preserve for appellate review the documents used to refresh the witness' recollection in violation of his statutory right to appellate review and his constitutional right to due process.

The state does not contest the fact that the defendant is entitled to see whatever Rovella used to refresh his recollection. Rather, the state first claims that it was the defendant's responsibility to voice his interest in a timely manner and that his failure to do so left the witness unable to identify definitively which reports of the many that he had prepared helped to refresh his recollection. Next, the state argues that the reason a trial court must allow an item to be marked for identification is to allow a reviewing court to assess the propriety of the trial court's ruling denying its admission into evidence. According to the state, because no attempt to offer evidence was made herein, the purpose behind the rule is not served and hence the rule is not applicable.

We need not address the propriety of the trial court's denial of the defendant's request, nor the policy

behind marking documents for identification. On the basis of the record in this case, we conclude that the defendant \*846 was not harmed by the trial court's ruling. Rovella could not state with specificity which other document he had used to refresh his recollection. He could state, however, that it was a police report that he personally had authored. There has been no claim that any of Rovella's statements had not been disclosed pursuant to Practice Book § 40-13(a)(1).<sup>FN57</sup> Indeed, as the defendant stated at trial: “[D]uring the course of trial ... [the state's attorney] had offered me an opportunity to look at all the reports and he has permitted me to review the contents of his folder with regards to ... Rovella....” Accordingly, all of Rovella's \*\*961 reports previously had been disclosed to the defendant, thereby allowing him to preserve *any* claim in connection thereto for appellate review.

FN57. Practice Book § 40-13 provides in relevant part: “(a) Upon written request by a defendant filed in accordance with Section 41-5 and without requiring any order of the judicial authority, the prosecuting authority, subject to Section 40-40 et seq., shall promptly, but no later than forty-five days from the filing of the request, unless such time is extended by the judicial authority for good cause shown, disclose to the defendant the names and, subject to the provisions of subsections (g) and (h) of this section, the addresses of all witnesses that the prosecuting authority intends to call in his or her case in chief and shall additionally disclose to the defendant:

“(1) Any statements of the witnesses in the possession of the prosecuting authority or his or her agents, including state and local law enforcement officers, which statements relate to the subject matter about which each witness will testify....”

### III



Appellate Court of Connecticut.

STATE of Connecticut

v.

Robert ELECK.

No. 31581.

Argued May 31, 2011.

Decided Aug. 9, 2011.

**Background:** Defendant was convicted in the Superior Court, Judicial District of Stamford–Norwalk, White, J., of assault in the first degree by means of a dangerous instrument. Defendant appealed.

**Holding:** The Appellate Court, Bishop, J., held that defendant failed to authenticate authorship of certain electronic messages sent to him from State's witness's account on social networking website.

Affirmed.

West Headnotes

## [1] Criminal Law 110 661

110 Criminal Law

110XX Trial

110XX(C) Reception of Evidence

110k661 k. Necessity and scope of proof.

Most Cited Cases

The trial court has broad discretion in ruling on the admissibility of evidence.

## [2] Criminal Law 110 1153.1

110 Criminal Law

110XXIV Review

110XXIV(N) Discretion of Lower Court

110k1153 Reception and Admissibility of Evidence

110k1153.1 k. In general. Most Cited Cases

The trial court's ruling on evidentiary matters will be overturned only upon a showing of a clear abuse of the court's discretion.

## [3] Criminal Law 110 1144.12

110 Criminal Law

110XXIV Review

110XXIV(M) Presumptions

110k1144 Facts or Proceedings Not Shown by Record

110k1144.12 k. Reception of evidence. Most Cited Cases

## Criminal Law 110 1153.1

110 Criminal Law

110XXIV Review

110XXIV(N) Discretion of Lower Court

110k1153 Reception and Admissibility of Evidence

110k1153.1 k. In general. Most Cited Cases

Reviewing court will make every reasonable presumption in favor of upholding the trial court's evidentiary ruling, and upset it only for a manifest abuse of discretion.

## [4] Criminal Law 110 444.2

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.2 k. Necessity of authentication or foundation in general. Most Cited Cases

Authentication is a necessary preliminary to the introduction of most writings in evidence.

[5] Criminal Law 110 444.4

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.4 k. Sufficiency of evidence; standard of proof in general. Most Cited Cases

Criminal Law 110 444.5

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.5 k. Circumstantial evidence in general. Most Cited Cases

In general, a writing may be authenticated by a number of methods, including direct testimony or circumstantial evidence.

[6] Criminal Law 110 444.4

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.4 k. Sufficiency of evidence; standard of proof in general. Most Cited Cases

Criminal Law 110 736

110 Criminal Law

110XX Trial

110XX(F) Province of Court and Jury in General

110k733 Questions of Law or of Fact

110k736 k. Preliminary or introductory questions of fact. Most Cited Cases

There need only be a prima facie showing of authenticity of a writing to the court; once a prima facie showing of authorship is made to the court, the evidence, as long as it is otherwise admissible, goes to the jury, which will ultimately determine its authenticity.

[7] Courts 106 97(1)

106 Courts

106II Establishment, Organization, and Procedure

106II(G) Rules of Decision

106k88 Previous Decisions as Controlling or as Precedents

106k97 Decisions of United States Courts as Authority in State Courts

106k97(1) k. In general. Most Cited Cases

Where a state rule of evidence is similar to a federal rule, state court reviews the federal case law to assist interpretation of state rule.

[8] Criminal Law 110 444.20

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.20 k. Telecommunications. Most Cited Cases

**Witnesses 410** ➤ 406

410 Witnesses

410IV Credibility and Impeachment

410IV(E) Contradiction

410k406 k. Competency of contradictory evidence. Most Cited Cases

Defendant failed to authenticate authorship of certain electronic messages sent to him from State's witness's account on social networking website, and thus messages were not admissible to impeach witness's credibility; although witness admitted that the messages were sent from her account, she denied their authorship and suggested that her account had been "hacked" by a third party, medium was not characterized by a high degree of security, and content of communications at issue, including a suggestion of an acrimonious history between defendant and the author, was not sufficiently distinctive to establish witness's authorship.

**[9] Criminal Law 110** ➤ 444.18

110 Criminal Law

110XVII Evidence

110XVII(P) Documentary Evidence

110k444 Authentication and Foundation

110k444.18 k. Letters and notes. Most Cited Cases

The mere fact that a letter was sent and a reply received does not automatically authenticate the reply; circumstances must indicate that the reply probably came from the addressee of the letter. Code of Evidence, § 9-1(a).

**[10] Courts 106** ➤ 90(2)

106 Courts

106II Establishment, Organization, and Procedure

106II(G) Rules of Decision

106k88 Previous Decisions as Controlling or as Precedents

106k90 Decisions of Same Court or Co-Ordinate Court

106k90(2) k. Number of judges concurring in opinion, and opinion by divided court. Most Cited Cases

One panel of the Appellate Court, on its own, cannot overrule the precedent established by a previous panel's holding.

**\*\*819** William B. Westcott, for the appellant (defendant).

Timothy F. Costello, assistant state's attorney, with whom, on the brief, were David I. Cohen, state's attorney, and Joseph C. Valdes, assistant state's attorney, for the appellee (state).

BISHOP, BEACH and SULLIVAN, Js.

BISHOP, J.

**\*633** The defendant, Robert Eleck, appeals from the judgment of conviction, rendered after a jury trial, of assault in the first degree by means of a dangerous instrument in violation of General Statutes § 53a-59 (a)(1). On appeal, the defendant claims that (1) the trial court improperly failed to admit into evidence a document that properly was authenticated and (2) the statutory scheme mandating a nonsuspendable, five year minimum term of imprisonment violates his rights to equal protection and due process under the federal constitution. We affirm the judgment of the trial court.

The following facts, which the jury reasonably could have found, are relevant to this appeal. The defendant attended a party at 16 Charles Street in Norwalk in the early morning hours of December 9, 2007. All of the approximately twenty teens and young adults who attended were consuming alcoholic

beverages, and many were intoxicated. While inside the house, the defendant was involved in at least two verbal confrontations with one guest, Matthew Peacock. The defendant also conversed on several occasions with another guest, Simone Judway. Shortly after 2:30 a.m., outside the house, the defendant and Peacock engaged in a physical altercation that included punching and grappling. Three other guests, including Zachary Finch, joined the fight \*634 to help Peacock. When the combatants were separated, both Peacock and Finch discovered that they had suffered stab wounds.

The defendant subsequently was arrested and charged with assault in the first degree with a dangerous instrument in violation of § 53a-59 (a)(1) in connection with the injury to Peacock and assault in the second degree in violation of General Statutes § 53a-60 (a)(2) in connection with the injury to Finch. Following a trial to the jury, the defendant was convicted of assault in the first degree regarding the assault on Peacock and acquitted of assaulting Finch. Because the defendant's assault conviction involved the use of a dangerous instrument, he faced a mandatory minimum sentence of five years. He was, in fact, sentenced to the mandatory \*\*820 minimum sentence of five years incarceration with an additional ten years of special parole. This appeal followed. Additional facts and procedural history will be set forth as necessary.

## I

The defendant first claims that the court abused its discretion in excluding from evidence a printout from his Facebook account documenting electronic messages purportedly sent to him by Judway from her Facebook account.<sup>FN1</sup> We do not agree.

FN1. Facebook is a social networking website that allows private individuals to upload photographs and enter personal information and commentary on a password protected “profile.” An individual chooses a name

under which the Facebook profile will be listed (user name). Users create networks of “friends” by sending and accepting friend requests. Subject to privacy settings that each user can adjust, a user's friends can see aspects of the user's profile, including the user's list of friends, and can write comments that appear on the profile. Additionally, any Facebook user can send a private message to any other Facebook user in a manner similar to e-mail. The defendant's claim concerns the latter type of message.

The following additional facts and procedural history are relevant to our resolution of the defendant's claim. \*635 As a witness for the state, Judway offered key testimony that, prior to the physical altercation, the defendant had told her that “if anyone messes with me tonight, I am going to stab them.” Subsequently, during cross-examination, defense counsel sought to impeach Judway's credibility by asking her whether she had spoken with the defendant in person since the incident. She responded that she had seen the defendant in public but had not spoken to him in person, by telephone or by computer. Defense counsel then showed Judway a printout purporting to show an exchange of electronic messages between the defendant's Facebook account and another account under the user name “Simone Danielle.”<sup>FN2</sup> Judway identified the user name as her own, but denied sending the messages to the defendant.<sup>FN3</sup> She also testified that someone had “hacked” into her Facebook account and changed her password “two [to] three weeks” ago such that she had been unable to access it subsequently.

FN2. The document contains the following exchange of unaltered messages from April 28, 2009:

“Simone Danielle: Hey I saw you the other day and I just want to say nice bike.

“[The Defendant]: why would you wanna talk to me

“Simone Danielle: I'm just saying that you have a nice bike that's all. The past is the past.

“[The Defendant]: yup thanks

“Simone Danielle: No problems”

FN3. The defendant's counsel appears to have transposed the user name; she repeatedly referred to the user name as “Danielle Simone” although the user name that appears on the document is “Simone Danielle.” As stated in the transcript, counsel requested that Judway examine the document and then asked her: “This is your Facebook name; is that correct, ‘Danielle Simone’?” Judway responded, “Yes.” Thereafter, when defense counsel asked the defendant whether he had received Facebook messages from “Danielle Simone,” he corrected her, clarifying that he received the messages from “Simone Danielle.” Neither the state nor the defendant took issue with counsel's verbal miscue, either at the trial or in their appellate briefs, and the court did not mention it in ruling on the objection. In light of these facts, we conclude that the miscue has no bearing on our consideration of this appeal.

**\*636** On the following day, during the defendant's testimony, his counsel offered into evidence the defendant's Facebook printout containing messages purportedly from Judway. The state objected on the grounds that the authorship of the messages could not be authenticated and the document was irrelevant. In response, to **\*\*821** authenticate the document, the defendant testified that he downloaded and printed the exchange of messages directly from his own comput-

er. He also advanced testimony that he recognized the user name, “Simone Danielle,” as belonging to Judway because she had added him as a Facebook “friend” a short time before he received the message. He testified that the “Simone Danielle” profile contained photographs and other entries identifying Judway as the holder of that account. Finally, he testified that when he logged in to his Facebook account after the previous day's testimony, user “Simone Danielle” had removed him from her list of Facebook “friends.” The defendant's counsel then argued that based on this testimony and Judway's identification of her user name, there was a sufficient foundation to admit the document for the jury's consideration. The court, however, sustained the state's objection on the ground that the defendant had not authenticated that the messages were written by Judway herself. The defendant claims that this determination was improper.

[1][2][3] The following standard of review and principles of law govern our resolution of the defendant's claim. “[T]he trial court has broad discretion in ruling on the admissibility ... of evidence.... The trial court's ruling on evidentiary matters will be overturned only upon a showing of a clear abuse of the court's discretion.... We will make every reasonable presumption in favor of upholding the trial court's ruling, and ... upset it [only] for a manifest abuse of discretion.” (Internal quotation marks omitted.) *State v. Garcia*, 299 Conn. 39, 56–57, 7 A.3d 355 (2010).

[4][5][6] **\*637** “It is well established that [a]uthentication is ... a necessary preliminary to the introduction of most writings in evidence.... In general, a writing may be authenticated by a number of methods, including direct testimony or circumstantial evidence.... Both courts and commentators have noted that the showing of authenticity is not on a par with the more technical evidentiary rules that govern admissibility, such as hearsay exceptions, competency and privilege.... Rather, there need only be a prima facie showing of authenticity to the court.... Once a prima

facie showing of authorship is made to the court, the evidence, as long as it is otherwise admissible, goes to the jury, which will ultimately determine its authenticity.” (Internal quotation marks omitted.) *Id.*, at 57–58, 7 A.3d 355.

Codifying these principles, § 1–3(a) of the Connecticut Code of Evidence provides in relevant part: “Questions of admissibility generally. Preliminary questions concerning ... the admissibility of evidence shall be determined by the court.” Additionally, § 9–1(a) of the Connecticut Code of Evidence provides: “Requirement of authentication. The requirement of authentication as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the offered evidence is what its proponent claims it to be.” Where documents are not self-authenticating,<sup>FN4</sup> the prima facie \*638 showing of authenticity\*\*822 may be made in a variety of ways including, but not limited to, the following: “(1) A witness with personal knowledge may testify that the offered evidence is what its proponent claims it to be....(3) The trier of fact or an expert witness can authenticate a contested item of evidence by comparing it with preauthenticated specimens.... (4) The distinctive characteristics of an object, writing or other communication, when considered in conjunction with the surrounding circumstances, may provide sufficient circumstantial evidence of authenticity.” (Citations omitted.) Conn.Code Evid. § 9–1(a), commentary.

FN4. The defendant does not argue that the Facebook messages were self-authenticating. Typically, electronic messages do have self-identifying features. For example, e-mail messages are marked with the sender's e-mail address, text messages are marked with the sender's cell phone number, and Facebook messages are marked with a user name and profile picture. Nonetheless, given that such messages could be generated by a third party under the guise of the named sender, opinions from other jurisdictions have not

equated evidence of these account user names or numbers with self-authentication. Rather, user names have been treated as circumstantial evidence of authenticity that may be considered in conjunction with other circumstantial evidence. See, e.g., *Commonwealth v. Purdy*, 459 Mass. 442, 450, 945 N.E.2d 372 (2011) (evidence that electronic communication originates from e-mail or social networking website that bears purported author's name is not sufficient alone to authenticate it).

[7] Although we have not found any Connecticut appellate opinions directly on point regarding the authentication of electronic messages from social networking websites, we are aware that federal courts as well as sister jurisdictions have written on this subject. We know, as well, that “[w]here a state rule is similar to a federal rule we review the federal case law to assist our interpretation of our rule.” (Internal quotation marks omitted.) *Jacobs v. General Electric Co.*, 275 Conn. 395, 407, 880 A.2d 151 (2005). Rule 901 of the Federal Rules of Evidence is consistent with § 9–1(a) of the Connecticut Code of Evidence, except that rule 901(b) contains an additional list of illustrations. See *State v. Swinton*, 268 Conn. 781, 811 n. 28, 847 A.2d 921 (2004). Accordingly, it is helpful to consider relevant federal case law, as well as the opinions of sister states whose rules of evidentiary authentication are similar.

[8] The precise issue raised here is whether the defendant adequately authenticated the authorship of certain messages generated via Judway's Facebook account.<sup>FNS</sup> The need for authentication arises in this context \*639 because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their com-

puters and cell phones unattended. Additionally, passwords and website security are subject to compromise by hackers. Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship. See, e.g., *Commonwealth v. Williams*, 456 Mass. 857, 869, 926 N.E.2d 1162 (2010) (admission of MySpace<sup>FN6</sup> message was error where proponent advanced no circumstantial evidence as to security of MySpace page or purported author's exclusive access).

FN5. In regard to authenticity, the state did not question whether the printout was a true and accurate copy, nor did it dispute that Judway held and managed the Facebook account from which the messages were sent.

FN6. MySpace, like Facebook, is a social networking website.

As a word of caution, however, we note that some have opined that the present lexicon and body of rules for authenticating the authorship of traditional documents is adequate with respect to electronic documents.<sup>FN7</sup> See P. Grimm et al., “Back \*\*823 to the Future: *Lorraine v. Markel American Insurance Co.* and New Findings on the Admissibility of Electronically Stored Information,” 42 Akron L.Rev. 357,362 (2009). As Pennsylvania's intermediate appellate court articulated in a case similar to the present one, “[the] appellant would \*640 have us create a whole new body of law just to deal with e-mails or instant messages.... However, the same uncertainties [that exist with electronic documents] exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of [the rules of evidence].... We see no justification for constructing unique rules for admissibility of electronic communications such as

instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.” (Citation omitted.) *In re F.P.*, 878 A.2d 91, 95–96 (Pa.Super.2005).

FN7. There are other issues concerning the admissibility of electronically stored information, however, that may test the limits of current rules more acutely. For example, in the case of a website that is frequently updated, issues may arise as to how to authenticate the content of the website as it appeared at a particular moment in the past. See *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 553 (D.Md.2007). Additionally, besides authentication issues, the evidentiary use of electronically stored information may raise novel issues regarding the rules on hearsay and original writings. See, e.g., *Connecticut Light & Power Co. v. Gilmore*, 289 Conn. 88, 116–17, 956 A.2d 1145 (2008) (articulating guidelines for the admissibility of printouts of electronic records under the business records exception).

We agree that the emergence of social media such as e-mail, text messaging and networking sites like Facebook may not require the creation of new rules of authentication with respect to authorship.<sup>FN8</sup> An electronic document may continue to be authenticated by traditional means such as the direct testimony of the purported author or circumstantial evidence of “distinctive characteristics” in the document that identify the author. See Conn.Code Evid. § 9–1(a), commentary.

FN8. That is not to say that it might not be useful to the orderly development of the law of evidence to investigate the appropriateness of new rules specifically pertaining to electronic evidence. It is enough to say at this

juncture that our present rules permit a reasoned determination of whether the document presently in question properly was excluded as inadequately authenticated.

Nevertheless, we recognize that the circumstantial evidence that tends to authenticate a communication is somewhat unique to each medium. For example, in the context of a telephone call, our Supreme Court has instructed that “[a] sufficient foundation is laid when \*641 the subject matter of the conversation, evidence of its occurrence, and prior and subsequent conduct of the parties fairly establish the identity of the person with whom conversation occurred.” *International Brotherhood of Electrical Workers Local 35 v. Commission on Civil Rights*, 140 Conn. 537, 547, 102 A.2d 366 (1953). Alternatively, this court held that the authorship of letters on a computer hard drive could be authenticated by the mode of expression of the writing, detailed references to the defendant's finances and circumstantial evidence linking the defendant's presence at home with the time the letters were created on his home computer. See *State v. John L.*, 85 Conn.App. 291, 298–302, 856 A.2d 1032, cert. denied, 272 Conn. 903, 863 A.2d 695 (2004). Specifically in the case of electronic messaging, Maryland's highest court has suggested that a proponent of a document might search the computer of the purported author for Internet history and stored documents or might seek authenticating information from the commercial host of the e-mail, cell phone messaging or social \*\*824 networking account. See *Griffin v. State*, 419 Md. 343, 363–64, 19 A.3d 415 (2011); see also *People v. Clevestine*, 68 A.D.3d 1448, 1450–51, 891 N.Y.S.2d 511 (2009) (authorship of MySpace messages authenticated where police retrieved record of conversations from victims' hard drive and MySpace officer testified that defendant had created the sending account), appeal denied, 14 N.Y.3d 799, 899 N.Y.S.2d 133, 925 N.E.2d 937 (2010).

In the present case, the defendant proffered evidence as to the accuracy of the copy and Judway's

connection to the Facebook account. He also proffered evidence that Judway had added him to her list of Facebook “friends” shortly before allegedly sending the messages, and then removed him as a friend after testifying against him at the trial. Specifically in regard to authorship, however, the direct testimony of the purported author, \*642 Judway, contradicted the defendant's assertion. While admitting that the messages were sent from her Facebook account, she simultaneously denied their authorship. She also suggested that she could not have authored the messages because the account had been “hacked.” Although this suggestion is dubious under the particular facts at hand, given that the messages were sent before the alleged hacking of the account took place, Judway's testimony highlights the general lack of security of the medium and raises an issue as to whether a third party may have sent the messages via Judway's account. Consequently, we agree with the trial court that the fact that Judway held and managed the account did not provide a sufficient foundation for admitting the printout, and it was incumbent on the defendant, as the proponent, to advance other foundational proof to authenticate that the proffered messages did, in fact, come from Judway and not simply from her Facebook account.

The defendant claims, nevertheless, that he did offer circumstantial evidence that Judway sent the messages. Specifically, he argues that the content of the messages identified Judway as the author. For example, when he sent the message asking “why would you wanna talk to me,” the other party replied, “The past is the past.” The defendant contends that this indicated that the author knew of the criminal case and, therefore, must have been Judway.

We are not convinced that the content of this exchange provided distinctive evidence of the interpersonal conflict between the defendant and Judway. To the contrary, this exchange could have been generated by any person using Judway's account as it does not reflect distinct information that only Judway

would have possessed regarding the defendant or the character of their relationship. In other cases in which a message has been held to be authenticated by its content, \*643 the identifying characteristics have been much more distinctive of the purported author and often have been corroborated by other events or with forensic computer evidence. See, e.g., *State v. John L.*, supra, 85 Conn.App. at 298–302, 856 A.2d 1032; see also *United States v. Siddiqui*, 235 F.3d 1318, 1322–23 (11th Cir.2000) (e-mails authenticated not only by defendant's e-mail address but also by inclusion of factual details known to defendant that were corroborated by telephone conversations), cert. denied, 533 U.S. 940, 121 S.Ct. 2573, 150 L.Ed.2d 737 (2001); *United States v. Tank*, 200 F.3d 627, 630–31 (9th Cir.2000) (author of chat room <sup>FN9</sup> message identified when he showed up at arranged meeting); *United States v. Safavian*, 435 F. Sup.2d 36, 40 (D.D.C.2006) (e-\*825 mail messages authenticated by distinctive content including discussions of various identifiable personal and professional matters); *Dickens v. State*, 175 Md.App. 231, 237–41, 927 A.2d 32 (2007) (threatening text messages received by victim on cell phone contained details few people would know and were sent from phone in defendant's possession at the time); *State v. Taylor*, 178 N.C.App. 395, 412–15, 632 S.E.2d 218 (2006) (text messages authenticated by expert testimony about logistics for text message receipt and storage and messages contained distinctive content, including description of car victim was driving); *In re F.P.*, supra, 878 A.2d at 93–95 (instant electronic messages authenticated by distinctive content including author's reference to self by name, reference to surrounding circumstances and threats contained in messages that were corroborated by subsequent actions); *Massimo v. State*, 144 S.W.3d 210, 215–17 (Tex.App.2004) (e-mails authenticated where e-mails discussed things only victim, defendant, and few others knew and written in way defendant \*644 would communicate). Compare *Griffin v. State*, supra, 419 Md. at 347–48, 19 A.3d 415 (admission of MySpace pages was reversible error where proponent advanced no circumstantial evidence of authorship).

Consequently, we conclude that the reference in the message to an acrimonious history, with nothing more, did not sufficiently establish that Judway authored the messages such that it would be an abuse of discretion to exclude the document.

FN9. A chat room is a public or private Internet site that allows individuals to send real time typed messages to others who are simultaneously connected to that Internet site.

[9] Finally, the defendant argues that the messages could be authenticated under the “reply letter” doctrine. We are not convinced. Under that doctrine, “letter *B* is authenticated merely by reference to its content and circumstances suggesting it was in reply to earlier letter *A* and sent by addressee of letter *A* ...” Conn.Code Evid. § 9–1(a), commentary (4). We note, however, that “[t]he mere fact that a letter was sent and a reply received does not automatically authenticate the reply; circumstances must indicate that the reply probably came from the addressee of the letter.” C. Tait & E. Prescott, *Connecticut Evidence* (4th Ed. 2008) § 9.7, p. 630; see also *Connecticut Limousine Service, Inc. v. Powers*, 7 Conn.App. 398, 401, 508 A.2d 836 (1986). Here, there was a lack of circumstantial evidence to verify the identity of the person with whom the defendant was messaging. Consequently, the reply letter doctrine is inapposite.<sup>FN10</sup>

FN10. We note that we need not and do not opine on the applicability of the reply letter doctrine to electronic messaging. See 2 C. McCormick, *Evidence* (6th Ed. 2006) § 227, p. 73.

We conclude, therefore, that the court did not abuse its discretion in declining to admit the document into evidence.

## II

[10] The defendant also claims that the statutory

scheme mandating a nonsuspendable, five year minimum term \*645 of imprisonment for a violation of § 53a-59 (a)(1) violates his rights to equal protection and due process under the federal constitution. Although he concedes that this court previously considered this claim in *State v. Schultz*, 100 Conn.App. 709, 726-29, 921 A.2d 595, cert. denied, 282 Conn. 926, 926 A.2d 668 (2007), in which we held that the statutory scheme is constitutional, the defendant asks this court to reconsider that decision. It is settled policy, however, that one panel of this court, on its own, cannot overrule the precedent established by a previous panel's holding. See \*\*826*First Connecticut Capital, LLC v. Homes of Westport, LLC*, 112 Conn.App. 750, 759, 966 A.2d 239 (2009). We decline, therefore, to consider the defendant's claim.

The judgment is affirmed.

In this opinion the other judges concurred.

Conn.App.,2011.

State v. Eleck

130 Conn.App. 632, 23 A.3d 818

END OF DOCUMENT

FEDERAL RULES  
OF  
EVIDENCE

---

DECEMBER 1, 2013



Printed for the use  
of  
THE COMMITTEE ON THE JUDICIARY  
HOUSE OF REPRESENTATIVES

## TABLE OF CONTENTS

Foreword .....	Page
Authority for promulgation of rules .....	III
Historical note .....	V
	VII

### RULES

Article I. General Provisions:	
Rule 101. Scope; definitions .....	1
Rule 102. Purpose .....	1
Rule 103. Rulings on evidence .....	1
Rule 104. Preliminary questions .....	2
Rule 105. Limiting evidence that is not admissible against other parties or for other purposes .....	2
Rule 106. Remainder of or related writings or recorded statements .....	2
Article II. Judicial Notice:	
Rule 201. Judicial notice of adjudicative facts .....	3
Article III. Presumptions in Civil Cases:	
Rule 301. Presumptions in civil cases generally .....	3
Rule 302. Applying State law to presumptions in civil cases .....	3
Article IV. Relevance and Its Limits:	
Rule 401. Test for relevant evidence .....	3
Rule 402. General admissibility of relevant evidence .....	4
Rule 403. Excluding relevant evidence for prejudice, confusion, waste of time, or other reasons .....	4
Rule 404. Character evidence; crimes or other acts .....	4
Rule 405. Methods of proving character .....	5
Rule 406. Habit; routine practice .....	5
Rule 407. Subsequent remedial measures .....	5
Rule 408. Compromise offers and negotiations .....	5
Rule 409. Offers to pay medical and similar expenses .....	6
Rule 410. Pleas, plea discussions, and related statements .....	6
Rule 411. Liability insurance .....	6
Rule 412. Sex-offense cases: the victim's sexual behavior or predisposition ..	7
Rule 413. Similar crimes in sexual-assault cases .....	7
Rule 414. Similar crimes in child-molestation cases .....	8
Rule 415. Similar acts in civil cases involving sexual assault or child molestation .....	9
Article V. Privileges:	
Rule 501. Privilege in general .....	9
Rule 502. Attorney-client privilege and work product; limitations on waiver	9
Article VI. Witnesses:	
Rule 601. Competency to testify in general .....	10
Rule 602. Need for personal knowledge .....	10
Rule 603. Oath or affirmation to testify truthfully .....	10
Rule 604. Interpreter .....	11
Rule 605. Judge's competency as a witness .....	11
Rule 606. Juror's competency as a witness .....	11
Rule 607. Who may impeach a witness .....	11
Rule 608. A witness's character for truthfulness or untruthfulness .....	11
Rule 609. Impeachment by evidence of a criminal conviction .....	12
Rule 610. Religious beliefs or opinions .....	13
Rule 611. Mode and order of examining witnesses and presenting evidence ..	13

Article VI. Witnesses—Continued	Page
Rule 612. Writing used to refresh a witness's memory .....	13
Rule 613. Witness's prior statement .....	14
Rule 614. Court's calling or examining a witness .....	14
Rule 615. Excluding witnesses .....	14
Article VII. Opinions and Expert Testimony:	
Rule 701. Opinion testimony by lay witnesses .....	15
Rule 702. Testimony by expert witnesses .....	15
Rule 703. Bases of an expert's opinion testimony .....	15
Rule 704. Opinion on an ultimate issue .....	15
Rule 705. Disclosing the facts or data underlying an expert's opinion .....	16
Rule 706. Court-appointed expert witnesses .....	16
Article VIII. Hearsay:	
Rule 801. Definitions that apply to this article; exclusions from hearsay .....	16
Rule 802. The rule against hearsay .....	17
Rule 803. Exceptions to the rule against hearsay—regardless of whether the declarant is available as a witness .....	17
Rule 804. Exceptions to the rule against hearsay—when the declarant is unavailable as a witness .....	21
Rule 805. Hearsay within hearsay .....	22
Rule 806. Attacking and supporting the declarant's credibility .....	22
Rule 807. Residual exception .....	22
Article IX. Authentication and Identification:	
Rule 901. Authenticating or identifying evidence .....	23
Rule 902. Evidence that is self-authenticating .....	24
Rule 903. Subscribing witness's testimony .....	25
Article X. Contents of Writings, Recordings, and Photographs:	
Rule 1001. Definitions that apply to this article .....	26
Rule 1002. Requirement of the original .....	26
Rule 1003. Admissibility of duplicates .....	26
Rule 1004. Admissibility of other evidence of content .....	26
Rule 1005. Copies of public records to prove content .....	27
Rule 1006. Summaries to prove content .....	27
Rule 1007. Testimony or statement of a party to prove content .....	27
Rule 1008. Functions of the court and jury .....	27
Article XI. Miscellaneous Rules:	
Rule 1101. Applicability of the rules .....	27
Rule 1102. Amendments .....	28
Rule 1103. Title .....	28

## FEDERAL RULES OF EVIDENCE

Effective July 1, 1975, as amended to December 1, 2013

### ARTICLE I. GENERAL PROVISIONS

#### Rule 101. Scope; Definitions

(a) SCOPE. These rules apply to proceedings in United States courts. The specific courts and proceedings to which the rules apply, along with exceptions, are set out in Rule 1101.

(b) DEFINITIONS. In these rules:

- (1) “civil case” means a civil action or proceeding;
- (2) “criminal case” includes a criminal proceeding;
- (3) “public office” includes a public agency;
- (4) “record” includes a memorandum, report, or data compilation;
- (5) a “rule prescribed by the Supreme Court” means a rule adopted by the Supreme Court under statutory authority; and
- (6) a reference to any kind of written material or any other medium includes electronically stored information.

(As amended Mar. 2, 1987, eff. Oct. 1, 1987; Apr. 25, 1988, eff. Nov. 1, 1988; Apr. 22, 1993, eff. Dec. 1, 1993; Apr. 26, 2011, eff. Dec. 1, 2011.)

#### Rule 102. Purpose

These rules should be construed so as to administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

#### Rule 103. Rulings on Evidence

(a) PRESERVING A CLAIM OF ERROR. A party may claim error in a ruling to admit or exclude evidence only if the error affects a substantial right of the party and:

- (1) if the ruling admits evidence, a party, on the record:
  - (A) timely objects or moves to strike; and
  - (B) states the specific ground, unless it was apparent from the context; or
- (2) if the ruling excludes evidence, a party informs the court of its substance by an offer of proof, unless the substance was apparent from the context.

(b) NOT NEEDING TO RENEW AN OBJECTION OR OFFER OF PROOF. Once the court rules definitively on the record—either before or at trial—a party need not renew an objection or offer of proof to preserve a claim of error for appeal.

(c) COURT’S STATEMENT ABOUT THE RULING; DIRECTING AN OFFER OF PROOF. The court may make any statement about the character or form of the evidence, the objection made, and the ruling.

The court may direct that an offer of proof be made in question-and-answer form.

(d) **PREVENTING THE JURY FROM HEARING INADMISSIBLE EVIDENCE.** To the extent practicable, the court must conduct a jury trial so that inadmissible evidence is not suggested to the jury by any means.

(e) **TAKING NOTICE OF PLAIN ERROR.** A court may take notice of a plain error affecting a substantial right, even if the claim of error was not properly preserved.

(As amended Apr. 17, 2000, eff. Dec. 1, 2000; Apr. 26, 2011, eff. Dec. 1, 2011.)

#### **Rule 104. Preliminary Questions**

(a) **IN GENERAL.** The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.

(b) **RELEVANCE THAT DEPENDS ON A FACT.** When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.

(c) **CONDUCTING A HEARING SO THAT THE JURY CANNOT HEAR IT.** The court must conduct any hearing on a preliminary question so that the jury cannot hear it if:

- (1) the hearing involves the admissibility of a confession;
- (2) a defendant in a criminal case is a witness and so requests; or
- (3) justice so requires.

(d) **CROSS-EXAMINING A DEFENDANT IN A CRIMINAL CASE.** By testifying on a preliminary question, a defendant in a criminal case does not become subject to cross-examination on other issues in the case.

(e) **EVIDENCE RELEVANT TO WEIGHT AND CREDIBILITY.** This rule does not limit a party's right to introduce before the jury evidence that is relevant to the weight or credibility of other evidence.

(As amended Mar. 2, 1987, eff. Oct. 1, 1987; Apr. 26, 2011, eff. Dec. 1, 2011.)

#### **Rule 105. Limiting Evidence That Is Not Admissible Against Other Parties or for Other Purposes**

If the court admits evidence that is admissible against a party or for a purpose—but not against another party or for another purpose—the court, on timely request, must restrict the evidence to its proper scope and instruct the jury accordingly.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

#### **Rule 106. Remainder of or Related Writings or Recorded Statements**

If a party introduces all or part of a writing or recorded statement, an adverse party may require the introduction, at that time, of any other part—or any other writing or recorded statement—that in fairness ought to be considered at the same time.

(4) admitting it will best serve the purposes of these rules and the interests of justice.

(b) NOTICE. The statement is admissible only if, before the trial or hearing, the proponent gives an adverse party reasonable notice of the intent to offer the statement and its particulars, including the declarant's name and address, so that the party has a fair opportunity to meet it.

(Added Apr. 11, 1997, eff. Dec. 1, 1997; amended Apr. 26, 2011, eff. Dec. 1, 2011.)

#### ARTICLE IX. AUTHENTICATION AND IDENTIFICATION

##### Rule 901. Authenticating or Identifying Evidence

(a) IN GENERAL. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) EXAMPLES. The following are examples only—not a complete list—of evidence that satisfies the requirement:

(1) *Testimony of a Witness with Knowledge*. Testimony that an item is what it is claimed to be.

(2) *Nonexpert Opinion About Handwriting*. A nonexpert's opinion that handwriting is genuine, based on a familiarity with it that was not acquired for the current litigation.

(3) *Comparison by an Expert Witness or the Trier of Fact*. A comparison with an authenticated specimen by an expert witness or the trier of fact.

(4) *Distinctive Characteristics and the Like*. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

(5) *Opinion About a Voice*. An opinion identifying a person's voice—whether heard firsthand or through mechanical or electronic transmission or recording—based on hearing the voice at any time under circumstances that connect it with the alleged speaker.

(6) *Evidence About a Telephone Conversation*. For a telephone conversation, evidence that a call was made to the number assigned at the time to:

(A) a particular person, if circumstances, including self-identification, show that the person answering was the one called; or

(B) a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.

(7) *Evidence About Public Records*. Evidence that:

(A) a document was recorded or filed in a public office as authorized by law; or

(B) a purported public record or statement is from the office where items of this kind are kept.

(8) *Evidence About Ancient Documents or Data Compilations*. For a document or data compilation, evidence that it:

(A) is in a condition that creates no suspicion about its authenticity;

(B) was in a place where, if authentic, it would likely be:  
and

(C) is at least 20 years old when offered.

(9) *Evidence About a Process or System.* Evidence describing a process or system and showing that it produces an accurate result.

(10) *Methods Provided by a Statute or Rule.* Any method of authentication or identification allowed by a federal statute or a rule prescribed by the Supreme Court.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

#### **Rule 902. Evidence That Is Self-Authenticating**

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

(1) *Domestic Public Documents That Are Sealed and Signed.* A document that bears:

(A) a seal purporting to be that of the United States; any state, district, commonwealth, territory, or insular possession of the United States; the former Panama Canal Zone; the Trust Territory of the Pacific Islands; a political subdivision of any of these entities; or a department, agency, or officer of any entity named above; and

(B) a signature purporting to be an execution or attestation.

(2) *Domestic Public Documents That Are Not Sealed but Are Signed and Certified.* A document that bears no seal if:

(A) it bears the signature of an officer or employee of an entity named in Rule 902(1)(A); and

(B) another public officer who has a seal and official duties within that same entity certifies under seal—or its equivalent—that the signer has the official capacity and that the signature is genuine.

(3) *Foreign Public Documents.* A document that purports to be signed or attested by a person who is authorized by a foreign country's law to do so. The document must be accompanied by a final certification that certifies the genuineness of the signature and official position of the signer or attester—or of any foreign official whose certificate of genuineness relates to the signature or attestation or is in a chain of certificates of genuineness relating to the signature or attestation. The certification may be made by a secretary of a United States embassy or legation; by a consul general, vice consul, or consular agent of the United States; or by a diplomatic or consular official of the foreign country assigned or accredited to the United States. If all parties have been given a reasonable opportunity to investigate the document's authenticity and accuracy, the court may, for good cause, either:

(A) order that it be treated as presumptively authentic without final certification; or

(B) allow it to be evidenced by an attested summary with or without final certification.

(4) *Certified Copies of Public Records.* A copy of an official record—or a copy of a document that was recorded or filed in

a public office as authorized by law—if the copy is certified as correct by:

(A) the custodian or another person authorized to make the certification; or

(B) a certificate that complies with Rule 902(1), (2), or (3), a federal statute, or a rule prescribed by the Supreme Court.

(5) *Official Publications*. A book, pamphlet, or other publication purporting to be issued by a public authority.

(6) *Newspapers and Periodicals*. Printed material purporting to be a newspaper or periodical.

(7) *Trade Inscriptions and the Like*. An inscription, sign, tag, or label purporting to have been affixed in the course of business and indicating origin, ownership, or control.

(8) *Acknowledged Documents*. A document accompanied by a certificate of acknowledgment that is lawfully executed by a notary public or another officer who is authorized to take acknowledgments.

(9) *Commercial Paper and Related Documents*. Commercial paper, a signature on it, and related documents, to the extent allowed by general commercial law.

(10) *Presumptions Under a Federal Statute*. A signature, document, or anything else that a federal statute declares to be presumptively or prima facie genuine or authentic.

(11) *Certified Domestic Records of a Regularly Conducted Activity*. The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)–(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them.

(12) *Certified Foreign Records of a Regularly Conducted Activity*. In a civil case, the original or a copy of a foreign record that meets the requirements of Rule 902(11), modified as follows: the certification, rather than complying with a federal statute or Supreme Court rule, must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed. The proponent must also meet the notice requirements of Rule 902(11).

(As amended Mar. 2, 1987, eff. Oct. 1, 1987; Apr. 25, 1988, eff. Nov. 1, 1988; Apr. 17, 2000, eff. Dec. 1, 2000; Apr. 26, 2011, eff. Dec. 1, 2011.)

### Rule 903. Subscribing Witness's Testimony

A subscribing witness's testimony is necessary to authenticate a writing only if required by the law of the jurisdiction that governs its validity.

(As amended Apr. 26, 2011, eff. Dec. 1, 2011.)

## PRELIMINARY SELECTED BIBLIOGRAPHY

Bellin, Jeffrey, Ehearsay, 98 Minn. L. Rev. 7 (2013).

Bergman, Kristin, Cyborgs in the Courtroom: The Use of Google Glass Recordings in Litigation, 20 Rich. J.L. & Tech. 11 (2014).

Carter, Pamela W. and Napolitano, Shelley K., Social Media: An Effective Evidentiary Tool, 61 La. B.J. 332 (2014).

Diaz, Adam Alexander, “Getting Information Off the Internet is Like Taking a Drink From a Fire Hydrant” – The Murky Area of Authenticating Website Screenshots in the Courtroom, 37 Am. J. Tr. Advocacy 65 (2013).

Frieden Jonathan D. and Murray, Leigh M., The Admissibility of Electronic Evidence Under the Federal Rules of Evidence, 17 Rich. J.L. & Tech. 5 (2010).

Finkelstein, Sheldon M. and Storch, Evelyn R., Admissibility of Electronically Stored Information: It’s Still the Same Old Story, J. Am. Acad. Matrim. Law. 45 (2010).

Grimm, Paul W., Bergstrom, Lisa Yurwit and O’Toole-Loureiro, Melissa M., Authentication of Social Media Evidence, 36 Am. J. Trial Advoc. 433 (2013).

Magnuson, Neil C. and Borden, Bennett B., The Admissibility of Digital Evidence: The \$64 Billion Question in *Ceglia v. Facebook*, 8 No.2 ABA SciTech Law. 4 (2011).

McPartland, Molly D., An Analysis of Facebook Likes and Other Nonverbal Internet Communicatiijn Under thre Federal Rules of Evidence, 99 Iowa L. Rev. 445 (2013).

Moore. Jonathan L., Time for an Upgrade: The Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation, 50 Jurimetrics J. 147 (2010).

Pannozzo, Allison L., Uploading Guilt: Adding a Virtual Records Exception to the Federal Rules of Evidence, 44 Conn. L. Rev. 1695 (2012).

Richter, Liesa L., Don’t Just Do Something!: E-Hearsay, The Present Sense Impression, and the Case for Caution in the Rulemaking Process, 61 Am. U. L. Rev. 1657 (2012).

Teppler, Steven W., Testable Reliability: A Modernized Approach to ESI Admissbility, 12 Ave Maria L. Rev. 213 (2014).

