Chapter 16. Trial Practice Management

By Kenneth N. Rashbaum*

Research References

West's Key Number Digest, Federal Civil Procedure 1311, 1551, 1921, 1922

eDiscovery and Digital Evidence §§6:16, 7:11, 14:10, 14:11

16:1. Introduction

While the overwhelming majority of trials settle before verdict in the current litigation environment, many cases proceed to a stage of trial, or are disposed by summary judgment motions that may require support by proof in admissible form. Much of that proof is electronic at present, though many lawyers are still accustomed to trying cases that rely on paper documents despite the fact that the business world has largely converted to electronic communications and data. It is easy, then, to overlook several critical differences between preparing cases for trial that depend on paper documents and preparing cases for trial that involve electronically stored information (ESI). First, mandatory disclosure obligations impact ESI differently than they did paper documents. Second, a trial may be significantly affected by sanctions such as adverse inferences or evidence preclusion resulting from the spoliation of ESI. Finally, a number of unique issues affect the admissibility of ESI at trial, including authentication and satisfaction of the original writing rule. As a result, litigators should become familiar with the issues that uniquely affect the use of ESI as evidence at trial, and ensure that such evidence is handled from the very outset of the case with an eye toward its potential use at trial.

16:2. Mandatory disclosures

Pursuant to the Federal Rules of Civil Procedure, parties are required to voluntarily and automatically disclose certain information relevant to the matter. Federal Rule of Civil Procedure 26(a) contains these obligations, which include specific requirements for initial disclosures, expert disclosures, and pretrial disclosures.

Initial Disclosures

Federal Rule of Civil Procedure 26(a)(1)(B) requires that parties automatically disclose "all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment."[1] The Rule's requirements on initial disclosures are intended to provide sufficient information to "enable opposing parties (1) to make an informed decision concerning which documents might need to be examined, at least initially, and (2) to frame their document requests in a manner likely to avoid squabbles resulting from the wording of the requests."[2] As such, there are several cautionary points worth noting with regard to initial disclosures and ESI.

---

* The author and editors gratefully acknowledge the contribution of the Honorable Paul Grimm (D. Md.) for the foundational development of this chapter and Carolin Brucker, LL.M. of Barton LLP (admitted to the Bar in Germany only) for assistance in updating and editing this chapter.

[1] Fed. R. Civ. P. 26(a)(1)(B).

[2] Fed. R. Civ. P. 26, Advisory Committee's Notes.

The first is that inadequate initial disclosures may result in evidence preclusion. Federal Rule of Civil Procedure 26(a)(1)(B) requires a party to disclose a general description of documents by category and location. This fact often results in very general disclosures that may lead a party to omit materials that are necessary for the claims or defenses at trial, making the disclosure inadequate. Importantly, pursuant to F.R.C.P. 37, any failure to make adequate disclosures under F.R.C.P. 26(a)(1), "unless the failure was substantially justified or is harmless" may result in having the information that was not disclosed prohibited from use as "evidence at a trial, at a hearing, or on motion."[3]

The second concern is the risk of overbroad disclosure. Before the 2000 amendments to the F.R.C.P., each party was required to disclose documents "relevant to disputed facts alleged with particularity in the pleadings," whether or not they were favorable to the disclosing party, or the disclosing party anticipated using them in its own case in chief.[4] Despite the fact that these rules have since changed to limit the breadth of disclosure, many attorneys still make disclosures that are overly broad, identifying more information than is necessary and inviting discovery into areas that might otherwise not be pursued.[5]

To determine what ESI must be disclosed in order to comply with F.R.C.P. 26(a)(1)(B), counsel should confer with their client to determine what of his/her electronic information is available, not only in active data stores, but also in back-up, legacy, and archival repositories.[6] Having identified potential sources of data, counsel should then make a good faith determination about what data will likely be used in support of their client's claims or defenses.[7] Furthermore, having made the initial determination with regard to what information must be disclosed, counsel should endeavor to supplement the initial disclosures to the extent that additional data may be identified as discovery progresses.[8] Finally, counsel should also remember to remove from the disclosure previously identified documents and ESI that he/she has determined will not be used in support of the client's claims or defenses.

Expert Disclosures

---

[3] Fed. R. Civ. P. 37(c)(1). *See* Caraustar Industries, Inc. v. North Georgia Converting, Inc., 2006 WL 3751453, *8 (W.D. N.C. 2006) (striking declaration filed in support of motion for summary judgment because, inter alia, the declarant and tests discussed in declaration had never been identified in Rule 26(a)(1) disclosures). This provision highlights the fact that initial disclosures should contemplate information that may be used in support of claims or defenses not only at trial, but at any phase of the litigation, including motion practice.

[4] Fed. R. Civ. P. 26, Advisory Committee's Notes.

[5] *See, e.g.,* Robinson v. Moran, 2007 WL 2915620, *3-5 (C.D. Ill. 2007) (denying motion for sanctions for failure to disclose printed timeline of electronically stored information regarding events in corrections facility where "there has been no showing that Defendants ... intend to *use* the timeline in any way") (emphasis in original).

[6] Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432-433 (S.D. N.Y. 2004).

[7] Fed. R. Civ. P. 26, Advisory Committee's Notes.

[8] *See, e.g.,* Tobias v. Davidson Plywood, 241 F.R.D. 590, 591–594 (E.D. Tex. 2007) (striking worker's compensation defense where defendant failed to disclose existence of worker's compensation policy pursuant to Rule 26(a)(1) and court order).

Pursuant to Federal Rule of Civil Procedure Rule 26(a)(2)(B), parties must disclose certain information regarding experts retained to offer opinion testimony at trial, including a report containing all of the expert's opinions.[9] The report must also identify "the data or other information considered by the witness in forming the opinions."[10] Parties proffering expert witnesses, however, must be careful to handle the production of reports and underlying data appropriately.

Counsel must be mindful of whether a draft report must be disclosed. As virtually all experts create their written reports on computers using word processors or other programs that easily retain copies, it is commonplace to receive requests for production of draft reports by experts. Courts, however, are split on whether experts have a responsibility to retain draft reports. At least one court has held that destruction of draft reports and associated communications constitutes spoliation of evidence, warranting adverse inference instructions and an award of attorney fees and costs.[11] Conversely, other courts have held that F.R.C.P. 26(a)(2) does not impose upon an independent expert a duty to preserve draft reports, or even communications with counsel.[12] Nevertheless, counsel must be aware of any discovery that would arguably call for the production of draft reports and, upon receipt, notify testifying experts to retain such drafts separately.

Pretrial Disclosures

Counsel must also be mindful during pretrial disclosures of ESI that may be used at trial as evidence. Federal Rule of Civil Procedure 26(a)(3) requires each party to "provide to other parties and promptly file with the court [certain] information regarding the evidence that it may present at trial other than solely for impeachment," including the names of witnesses to be presented by deposition or live, and "an identification of each document or other exhibit, including summaries of other evidence ...."[13] These disclosures must be made at least 30 days prior to trial or as ordered by the court. Within 14 days of these pretrial disclosures, other parties

---

[9] Fed. R. Civ. P. 26(a)(2)(B).

[10] Fed. R. Civ. P. 26(a)(2)(B).

[11] *See, e.g.,* Trigon Ins. Co. v. U.S., 204 F.R.D. 277, 57 Fed. R. Evid. Serv. 664, 51 Fed. R. Serv. 3d 378 (E.D. Va. 2001).

[12] *See* University of Pittsburgh v. Townsend, 2007 WL 1002317, *3-5 (E.D. Tenn. 2007) ("the Court does not read Rule 26(a)(2) to impose an 'affirmative duty' upon an expert to preserve 'all documents,' particularly report drafts, and the defendants do not cite any support for such a sweeping obligation"; the court also noted, however, that such materials should not have been destroyed if there were pending discovery requests for them); Bedford, LLC v. Safeco Ins. Co., 136 Wash. App. 1013, 2006 WL 3616434, *4 (Div. 1 2006) (affirming trial court's holding that there is "no legal principle that would require a testifying expert to separately retain all electronic drafts, including those that were overridden [sic] or subsumed during the drafting process") (emphasis in original).

[13] Fed. R. Civ. P. 26(a)(3).

must file any objections to any of the disclosed witnesses, depositions, or exhibits.[14] Both disclosures and objections under F.R.C.P. 26(a)(3) can be critical to a party's trial presentation.

Although the 2006 amendments did not modify F.R.C.P. 26(a)(3), it is beyond dispute that pretrial disclosures under F.R.C.P. 26(a)(3) must address ESI.[15] As such, counsel must ensure that they disclose both the ESI that they anticipate will be used at trial and the sponsoring witnesses for that ESI. Similarly, counsel should be vigilant when reviewing pretrial disclosures, especially with regard to ESI as trial evidence and sponsoring witnesses, as the failure to object to witnesses or exhibits identified in pretrial disclosures may waive any objections to such testimony or evidence other than those under Federal Rules of Evidence 402 and 403, unless excused by the court.[16]

16:3. Discovery sanctions

Courts have continued to invoke their inherent power to issue sanctions such as adverse inference instructions and to limit use of evidence pursuant to F.R.C.P. 37, though sanctions under the new Rule 37(e) will diminish while not entirely fading. From 2000 to 2012, the number of written opinions in federal cases in which sanctions for eDiscovery violations were addressed rose approximately from six[1] to 120, reaching its peak in 2011 at 150 cases.[2] Of the 120 reported cases in 2012 addressing eDiscovery sanctions, the court awarded sanctions in 69 cases (57.5%) of cases.[3] Specifically, monetary sanctions were granted in 44 cases, adverse inferences were granted in 20 cases, 10 cases precluded the admission of evidence, 5 cases granted terminating sanctions, and 14 cases granted sanctions classified as other.[4]

The tortuous history of sanctions for failure to preserve ESI may have ended with the adoption of Fed. R. Civ. P. 37(e), though litigation about sanctions is bound to continue. The

---

[14] Fed. R. Civ. P. 26(a)(3).

[15] *See* Fed. R. Civ. P. 26, Advisory Committee's Notes ("The disclosure obligation attaches both to witnesses and documents a party intends to use and also to witnesses and to documents the party intends to use if—in the language of Rule 26(a)(3)—'the need arises.'").

[16] Fed. R. Civ. P. 26; *see, e.g.,* Phillips v. Morbark, Inc., 519 F. Supp. 2d 591, 595-597 (D.S.C. 2007) (denying plaintiffs' motion for JNOV or new trial based, in part, on admission of videotape where the videotape had been disclosed on both the defendant's and plaintiffs' Rule 26(a)(3) pretrial disclosures).

[1] Dan H. Willoughby, Rose Hunter Jones and Gregory R. Antine, Sanctions for E-Discovery Violations: By The Numbers, Duke Law Journal, Nov. 15, 2010, available at http://legalworkshop.org/2010/11/15/sanctions-for-eDiscovery-violations-by-the-numbers.

[2] Gibson Dunn 2012 Year-End Electronic Discovery and Information Law Update, Jan. 14, 2013, available at http://gibsondunn.com/publications/pages/2012-YearEnd-Electronic-Discovery-Update.aspx.

[3] Gibson Dunn 2012 Year-End Electronic Discovery and Information Law Update, Jan. 14, 2013, available at http://gibsondunn.com/publications/pages/2012-YearEnd-Electronic-Discovery-Update.aspx.

[4] Gibson Dunn 2012 Year-End Electronic Discovery and Information Law Update, Jan. 14, 2013, available at http://gibsondunn.com/publications/pages/2012-YearEnd-Electronic-Discovery-Update.aspx.

Rule, effective December 1, 2015, removes an element of judicial discretion from the decision to impose sanctions, thus resolving inconsistencies across or even within districts. The Amended Rule 37(e) states:

Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court: (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may: (A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment.[5]

The new Rule thus requires courts to consider the cause of the loss of the information and the practical effects of loss of that ESI upon the underlying litigation. It states that the court, when faced with a motion for spoliation sanctions, must consider whether the information should have been preserved in anticipation of litigation; was "lost because a party failed to take reasonable steps to preserve it;" and it "cannot be restored or replaced through additional discovery."[6] If a court answers each of these questions in the affirmative, there are more hurdles. If the court finds prejudice to another party from the loss of the information, it "may order measures no greater than necessary to cure the prejudice."[7] However, if the court finds all of these factors plus "an intent to deprive another party of the information's use in the litigation," it *may* issue sanctions on one of these circumscribed categories: "(A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment."[8]

Yet, the opinions that preceded the adoption of the new Rule may live on as each side in a spoliation dispute may well claim one or more of the cases that follow as support for their position that a particular sanction should or should not lie in a given case. In addition, the Rule does not provide guidance as to reservation "triggers," i.e., when a party should have been preserved in anticipation of litigation, or whether the party who was to have produced the information took reasonable steps to preserve it, nor guidance on how to assess when more severe sanctions should be imposed.

For example, while Judge Scheindlin's analytical framework for the imposition of sanctions in *Pension Committee v. Banc of America* may have been largely abrogated by the

---

[5] A redlined version of Rule 37(e) is found at Proposed Amendments to the Federal Rules of Civil Procedure, Rules 1, 4, 16, 26, 30, 31, 33, 34, 37, 55, and 84 and the Appendix of Forms, Absent Contrary Congressional Action, 305 F.R.D. 457, 567-568 (2015).

[6] Fed. R. Civ. P. 37(e).

[7] Fed. R. Civ. P. 37(e)(1). *See* Snider v. Danfoss, LLC, 2017 WL 2973464 (N.D. Ill. 2017), report and recommendation adopted, 2017 WL 3268891 (N.D. Ill. 2017), in which defendant employer deleted plaintiff employee's emails as well as those of her acting supervisor. The court found no prejudice, in that the subject emails would have hurt the plaintiff's case and, in any event, similar evidence was available from another source.

[8] Fed. R. Civ. P. 37(e)(2).

Rule, a good deal of it will live on, such as an assessment of the degree of culpability, including questions of whether the alleged spoliator's conduct of discovery acceptable or was it negligent, grossly negligent, or willful. Yet, the Sixth Circuit wrote in *Lorie Applebaum v. Target* that "a showing of negligence or (even) gross negligence will not do the trick."[9] That said, question of who should bear the burden of proving that evidence has been lost or destroyed and the consequences resulting from that loss is in this framework and will remain a ripe area for dispute. Questions as to the appropriate remedy for the harm caused by the spoliation will also remain.[10]

Courts may continue to differ with regard to the mental state required to award sanctions,[11] and the burden of proof with regard to the relevance of the evidence.[12] To be sure, as then Chief Magistrate Judge Paul Grimm acknowledged in *Victor Stanley,* significant disparity has existed amongst the various federal circuits with regard to the imposition of sanctions for some time, leading to the adoption of the new Rule.[13] Some courts have taken the position that Rule 37(e) applies only to a failure to take reasonable steps to preserve information or to *prevent* its loss and that the Rule is *inapplicable* to intentional deletion of information, In *Hsueh v. New York State Department of Financial Services*,[14] the motion for an adverse instruction sanction

---

[9] Applebaum v. Target Corporation, 831 F.3d 740, 101 Fed. R. Evid. Serv. 35 (6th Cir. 2016).

[10] Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, 685 F. Supp. 2d 456, 463 (S.D. N.Y. 2010) (abrogated by, Chin v. Port Authority of New York & New Jersey, 685 F.3d 135 (2d Cir. 2012)). (The Second Circuit in *Chin* rejected the notion that a failure to institute a "litigation hold" constitutes gross negligence per se, abrogating *Pension Committee* in that regard. Instead, citing Orbit One Communications, Inc. v. Numerex Corp., 271 F.R.D. 429, 441 (S.D. N.Y. 2010) with approval, the court in *Chin* agreed that "the better approach is to consider [the failure to adopt good preservation practices] as one factor" in the determination of whether discovery sanctions should issue.) Judge Scheindlin also made it quite clear that, in the Southern District of New York, at least, expectations had risen since the federal rules were amended to address eDiscovery: "By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records—paper or electronic—and to search in the right places for those records, will inevitably result in the spoliation of evidence." Pension Commitee, 685 F.Supp.2d at 462.

[11] *Compare* Pension Committee, 685 F. Supp. 2d at 469 *with* Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) (quoting Russell v. University of Texas of Permian Basin, 234 Fed. Appx. 195, 208, 223 Ed. Law Rep. 612 (5th Cir. 2007); *but see* Paice LLC v. Hyundai Motor Co., 2015 WL 4984198 (D. Md. 2015) (refusing sanctions for deleting raw data not normally retained).

[12] *Compare* Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, 685 F. Supp. 2d at 469 *with* Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) (quoting Russell v. University of Texas of Permian Basin, 234 Fed. Appx. 195, 208, 223 Ed. Law Rep. 612 (5th Cir. 2007)).

[13] Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010).

[14] Hsueh v. New York State Department of Financial Services, 2017 WL 1194706 (S.D. N.Y. 2017). See also the inherent authority of state court judges to levy spoliation sanctions, Simons v. Petrarch LLC, 2017 WL 914631 (N.Y. Sup 2017), where plaintiff in a hostile workplace action

was granted where the plaintiff had admitted at deposition that she had intentionally deleted a recording with an individual form Human Resources. The court held that such issuance of sanctions was within its inherent authority and that that the court was not constrained by Rule 37 basis because that Rule does not apply to intentional deletion of evidence.

Rule 37(e)(2)(A) and (B) permit, with satisfaction of the criteria mentioned above, an adverse inference instruction as a sanction where the loss of information results in prejudice that cannot be remedied by additional discovery or other measures and where the alleged spoliating party intentionally lost the information; that is, "acted with an intent to deprive another of the use of the information."[15] For example, in *KCH Services, Inc. v. Vanaire, Inc.*, the court considered the questions of preservation trigger and intent to deprive the adverse party of the information and ordered an adverse inference instruction where the defendants deleted potentially relevant evidence from computers after having notice of possible and actual litigation.[16] Approximately one month before filing suit, the plaintiff informed the defendants by telephone that it thought they were using illegal copies of its software. Before the plaintiff filed suit, the defendants instructed their employees to delete any software from company computers that the company had not purchased. The defendants continued to delete and overwrite software even after the plaintiff filed its complaint and sent a preservation letter. The court noted that the obligation to preserve arises not when a party actually knows litigation is looming, but rather when the party "'should have known' that the information 'may be' relevant to future litigation."[17]

Although there was no question that the defendants were on notice after receiving the Complaint and preservation letter, the court found that, under the circumstances, they should have known when they received the initial telephone call.[18] Nevertheless, the court refused to enter terminating sanctions, holding that an adverse inference instruction would "fairly compensate the plaintiff for lost evidence that may have been presented to the jury."[19]

In *Flagg v. City of Detroit*, the Sixth Circuit affirmed the District Court's imposition of a permissive adverse inference in light of the parties conduct.[20] In that case, the relevant emails of two city employees were intentionally purged from the city's email system despite the court's preservation order. In discussing the appropriateness of the court's rebuttable adverse inference, the Sixth Circuit opined that, despite intentional conduct, a non-rebuttable adverse inference would be "tantamount to the entry of judgment" and therefore inappropriate in light of the facts of the case.[21]

Similarly, with regard to extreme sanction of dismissal, the court may dismiss a claim

---

deleted logs and other information but kept and produced edited versions of texts and other information. The court held that defendants were entitled to an adverse inference jury instruction.

[15] Fed. R. Civ. P. 37(e)(2).

[16] KCH Services, Inc. v. Vanaire, Inc., 2009 WL 2216601, *1 (W.D. Ky. 2009).

[17] KCH Services, Inc. v. Vanaire, Inc., 2009 WL 2216601, *4 (W.D. Ky. 2009).

[18] KCH Services, Inc. v. Vanaire, Inc., 2009 WL 2216601, *1 (W.D. Ky. 2009).

[19] KCH Services, Inc. v. Vanaire, Inc., 2009 WL 2216601, *2 (W.D. Ky. 2009).

[20] Flagg v. City of Detroit, 715 F.3d 165, 91 Fed. R. Evid. Serv. 263, 85 Fed. R. Serv. 3d 692 (6th Cir. 2013).

[21] Flagg v. City of Detroit, 715 F.3d 165, 178, 91 Fed. R. Evid. Serv. 263, 85 Fed. R. Serv. 3d 692 (6th Cir. 2013).

only where the party's conduct is "so egregious that he has forfeited his claims."[22] For instance, in *Taylor v. Mitre Corp*., an employment action, the court dismissed Taylor's claims as a sanction because Taylor had destroyed evidence by backing up his work computer to a laptop, destroying his work computer with a sledgehammer, and then running "specialized software to destroy data on his laptop so thoroughly that it cannot be recovered, even by forensic experts."[23]

The decisions on the scope of discovery sanction are, as perhaps one would expect, highly fact-specific and will depend, to a great extent, on the prejudice, if any, suffered by the requesting party.[24] The burden of proof as to prejudice will also continue to be hotly contested.[25] In *Arista Records v. Usenet.com, Inc.*, the defendants engaged in multiple acts of misconduct after litigation commenced, including wiping the hard drives of key players, giving terminated employees their computers as "parting gifts," and manipulating its systems to accelerate the overwriting of data relevant to the plaintiffs' copyright infringement claims.[26] Despite finding that the defendants acted in bad faith, the court rejected the request termination sanctions. Instead, the court held that the defendants would be precluded from relying on their primary affirmative defense, resulting in summary judgment in favor of the plaintiffs.[27]

In *Yelton v. PHI, Inc.*,[28] the defendant in a products liability action was sanctioned in the form of an adverse inference and an award of attorney fees for failing to include a researcher, who was hired after the triggering event to conduct a simulation of an accident, in its litigation hold. In the accident, a helicopter owned and operated by PHI was struck in the windshield by a red-tailed hawk, causing the helicopter to crash and killing all but one passenger. Both PHI and Sikorsky Aircraft, the manufacturer, were named as defendants. Shortly after issuing the litigation hold, Dr. Wonsub Kim was hired to conduct a simulated bird strike event on the aircraft involved in the accident. Dr. Kim was not advised of the litigation hold at the time he was hired. A year into the lawsuit, Dr. Kim was issued a new laptop and his old one, containing information regarding the analysis he conducted, was refreshed, causing a loss of information. Approximately two years after the lawsuit was commenced, Sikorsky "realized" it failed to include Dr. Kim in the litigation hold and corrected the mistake. The court found that at the time Dr. Kim was hired, after the accident but before the lawsuit, he was a "key player" because he was hired to conduct a simulation of the accident. Finding that spreadsheets, PowerPoints, Word documents, reports, and information were destroyed when Dr. Kim's laptop was refreshed, the court held that Sikorsky acted with "a significant degree of culpability," hinting that the

---

[22] Taylor v. Mitre Corp., 2012 WL 5473573, *3 (E.D. Va. 2012).

[23] Taylor v. Mitre Corp., 2012 WL 5473573, *3 (E.D. Va. 2012).

[24] *See* Core Laboratories LP v. Spectrum Tracer Services, L.L.C., 2016 WL 879324 (W.D. Okla. 2016), in which an adverse inference was ordered despite the absence of intent to deprive, where the evidence was critical.

[25] *Compare* Sekisui American Corp. v. Hart, 945 F. Supp. 2d 494 (S.D. N.Y. 2013); *with* Fleming v. Escort, Inc., 2015 WL 5611576, *2 (D. Idaho 2015) (burden is on the producing party to show lack of prejudice).

[26] Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 134-38 (S.D. N.Y. 2009).

[27] Arista Records LLC, 633 F. Supp. 2d at 159.

[28] Yelton v. PHI, Inc., 279 F.R.D. 377 (E.D. La. 2011), objections overruled, 284 F.R.D. 374 (E.D. La. 2012).

misconduct was intentional, and concluded that the logical inference was that the results of the analysis were not favorable to Sikorsky. The court awarded PHI sanctions in the form of both an adverse inference, to be crafted by the trial judge, and attorney fees and costs incurred due to the spoliation.[29]

Finally, in *Victory Stanley II*, Judge Grimm imposed more than $1 million in sanctions on the defendant for attorney fees and costs.[30] The judge explained that "t]his is because the effects of spoliation are not limited to a party's *efforts* to discover and to prove the spoliation and its scope. Rather, the willful loss or destruction of relevant evidence taints the entire discovery and motions practice." In this case specifically, the court found that "Defendants' first spoliation efforts corresponded with the beginning of litigation" and that "Defendants' misconduct affected the entire discovery process since the commencement of this case."[31] Similarly, in *In re Pradaxa,*the defendants were fined $931,500.00 for ongoing and repeated "egregious" discovery abuses such as the failure to issue a litigation hold as a "measured action, designed to let the defendants know that the Court's order and the Court deserve respect."[32] While the dollar amount of such sanctions may diminish under the new Rule, the criteria in the cases cited for imposing sanctions of any sort will remain a part of e-discovery jurisprudence.

16:4. Admissibility of evidence at trial

The admissibility of electronic evidence is the subject of numerous federal and state court opinions, most of which focus on traditional foundational requirements for evidence. That is to say that the party proffering ESI must establish its relevancy, authenticity, that the ESI does not constitute hearsay, and that the ESI satisfies the original writing rule. Relevancy, of course, is case specific. However, there are general principles that apply to authenticity, demonstrating that ESI is not hearsay, and satisfying the original writing rule.

16:5. Admissibility of evidence at trial—Authentication

Federal Rules of Evidence 901 through 903 are concerned with ensuring that ESI presented to a jury is what its proponent claims it to be.[1] While there is a requirement that a party offering evidence at trial lay a foundation from which a jury could conclude that evidence is what the party represents it to be, it "is not a particularly high barrier to overcome."[2] Even so, "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."[3]

---

[29] Yelton v. PHI, Inc., 279 F.R.D. 377 (E.D. La. 2011). The availability of costs and attorneys' fees as a sanction for spoliation after the effective date of Fed. R. Sic. P. 37(e) is unclear.

[30] Victor Stanley, Inc. v. Creative Pipe, Inc., 2011 WL 2552472, *2 (D. Md. 2011).

[31] Victor Stanley, Inc., 2011 WL 2552472, *2.

[32] In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation, 2014 WL 984911, *1 (S.D. Ill. 2014).

[1] Fed R. Evid. 901 to 903.

[2] Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 542, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).

[3] Lorraine, 241 F.R.D. at 542; *see also* Bowers v. Rector and Visitors of University of Va., 2007 WL 2963818 (W.D. Va. 2007), on reconsideration in part, 2008 WL 2346033 (W.D. Va. 2008).

To a great extent, the process of authentication of digital evidence will become much easier after December 1, 2017, when the amendment to FRE 901(14) takes effect—so long as proponents of the evidence follow the process laid out in the Rule. The new Rule states that electronic evidence will be self-authenticating (i.e., without the need to present other evidence of authenticity, in the manner of admission of certain public documents presently) if the evidence was collected by a process of digital identification and that process is certified in a written statement of a person qualified to attest to the fact that the information was collected with an authentication process "of digital identification." In other words, new Rule 902(14) can obviate the need to call live witnesses and present other evidence that the information is what the proponent represents it to be. But the rub, as Shakespeare said, is in the details and the details, in turn, pivot on the manner of collection[4] of the evidence in a way that preserves its "digital fingerprint," called a hash value. For evidence obtained in accordance with the Rule, this promises a sea change in admissibility foundation procedure that can save costs and time at trial.

The pertinent text of the amended Rule is as follows:

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:

***

(14) *Certified Data Copied from an Electronic Device, Storage Medium, or File.* Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12).[5]

Civil litigation, and much criminal litigation, depends on documentary evidence. Over 90 percent of all business documents are in digital format, and less than five percent of those documents are ever printed, so electronic documents and data comprise the vast majority of trial exhibits. A rule that eliminates the need to present extrinsic evidence such as live expert testimony in order to meet the requirement of proof of authentication of emails, texts, database reports and other forms of electronic evidence has obvious implications for the costs and time requirement of a trial. There are, though, a number of hurdles to be cleared before a party can reap the benefits of this new Rule.

The Rules Advisory Committee, in its Notes to the proposed amendment, indicated the rationale for bringing trial evidence practice into the 21st century by recognizing the unique identifiers in digital evidence and how they may obviate traditional means of authentication through live testimony:

Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value.' A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy

[4] "Copying" of digial evidence from an electronic device is used here interchangeably with the term "collection," as such copying is referenced by those who practice in the e-discovery arena.

[5] Fed. R. Evid. 902(14).

reliably attest to the fact that they are exact duplicates.[6]

The amendment, then, recognizes that the evidence itself, through its digital identifiers the hash values, can comprise sufficient indicia that the evidence is what it purports to be so that additional time-consuming testimony and documentary evidence should not be required.

But, as one may expect, merely demonstrating to the court the hash values of the proposed digital evidence is not sufficient to obtain the benefit of self-authentication under the new Rule. In order to avoid the time and expense of presenting live expert testimony, the proponent of the evidence must meet the criteria of the Rule. These include:

- "Copying" (collection) of the evidence from the subject device in a way that preserves the hash values.
- A certification of a qualified person as to that collection and the hash value identifiers pursuant to the Certification provisions of Rules 902 (11) or (12).[7]
- Appropriate qualifications of the person who has prepared and signed the Certification.

An offer of digital proof via new Rule 902(14) may be challenged on each of these grounds.[8] The Certification process pursuant to Rule 902(11), as referenced in new Rule 902 (14) "is a process by which a proponent seeking to introduce electronic data into evidence must present a certification in the form of a written affidavit that would be sufficient to establish authenticity were that information provided by a witness at trial."[9] Indeed, the Certification and the process in which it was obtained may be subject to challenge because it must be provided by a "'qualified person" who utilized best practices for the collection, preservation and verification of the digital evidence sought to be admitted."[10] This Rule will therefore frequently call into question electronic evidence collection methods that do not enable a defensible "digital identification" and verification process, perhaps through challenges under FRE 702, *Daubert v.*

---

[6] Fed. R. Evid. 902(14), advisory committee's note (2017).

[7] "This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology." Fed. R. Evid. 902(14), advisory committee's note (2017).

[8] *See* Patzakis, New Rule of Evidence to Directly Impact Computer Forensics and e-Discovery Preservation Best Practices (Dec. 6, 2016), https://blog.x1discovery.com/2016/12/06/new-federal-rule-of-evidence-to-directly-impact-computer-forensics-and-ediscovery-preservation-best-practices/ (last visited October 10, 2017).

[9] Patzakis, New Rule of Evidence to Directly Impact Computer Forensics and e-Discovery Preservation Best Practices.

[10] Patzakis, New Rule of Evidence to Directly Impact Computer Forensics and e-Discovery Preservation Best Practices.

Merrell-Dow Pharmaceuticals,[11] *People v. Frye*[12] or other means with regard to the methodology of the evidence collection, preservation of the hash values or qualifications of the person who signs the Certification. The Advisory Committee has explicitly noted the possibility of a "challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert."[13]

It is also important to remember, in regard to the above, that new Rule 902(14) creates only a presumption of authenticity. Challenges such as those cited above may rebut that presumption and the court may then require live testimony, including that of expert witnesses to establish the foundation for admission of the subject electronic evidence.

New Rule 902(14) proposes a streamlined means to admit electronic evidence that recognizes that the technology itself (hash value identifiers) can square the round hole into which the square peg of digital evidence was previously required to fit due to authentication rules that were somewhat outdated in the era of electronic information. Yet, that the Rules Advisory Committee gives it may take away in terms of motion and expert witness costs that will be incurred while advocates and courts grope their way through the interstices of the new Rule and interpreting its requirements. Evidence that was not collected in the forensically sound method that preserves the digital identifiers, or digital information that does not comprise these or similar identifiers[14] will be subject to the old rules of foundations for admissibility.

In the absence of hash values or other forms of electronic identification that meet the requirements of new Rule 902(14), the difficulty with authenticating ESI stems from the fact that proponents must, in essence, authenticate the computer itself as well as the data entry and retrieval processes to authenticate the resulting data.[15] Thus, it may be necessary for the "authenticating witness [to] 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

---

[11] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469, 37 Fed. R. Evid. Serv. 1 (1993).

[12] Frye v. U.S., 293 F. 1013, 34 A.L.R. 145 (App. D.C. 1923). States that still follow the general acceptance Frye standard for admissibility of expert testimony, as opposed to the standard enunciated in Daubert, supra, include Florida, Illinois, New Jersey New York and Washington, among others.

[13] Fed. R. Evid. 902(14), advisory committee's note (2017).

[14] The identifiers in the new Rule may not be limited to hash values, and may also comprise other means of identification that provide indicia of reliability form, perhaps a form of "future technology." Fed. R. Evid. 902(14), advisory committee's note (2017).

[15] *See* Lorraine, 241 F.R.D. at 544 ("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.") (quoting Weinstein's Federal Evidence §900.06[3] (2d ed) (hereafter "Weinstein")).

that does so."[16]

When identifying and collecting ESI parties should take steps to ensure that the process is well documented by someone who is familiar with the systems from which the data are collected and who can testify about the steps taken to preserve the data, and the reliability of the computer systems on which it was created and stored. If the ESI is processed for production (e.g., converted to an imaged format or stripped of metadata), the producing party may also need to offer foundational evidence that the production process did not alter relevant information contained in the ESI.

One way to authenticate ESI is through the use of hash values.[17] A hash value is, in simple terms, a unique numeric value that is assigned to ESI by a mathematical algorithm. The hash value can be assigned to a single file, a group of files, or an entire hard drive, and is said to be more precise than human DNA in distinguishing files.[18]

Often, courts require more than just the authentication of the computer file itself, which may well be represented at trial by a printout or even through the testimony of a witness. The specific requirements for authentication tend to vary widely in different courts, and "more courts have tended towards the lenient rather than the demanding approach" to authentication of ESI.[19]

Nevertheless, "it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied."[20]

Perhaps the most stringent standards that have been applied are the 11 criteria advocated by Professor Imwinkelried and adopted by the court in *In re Vee Vinhnee*.[21] In that case, the party proffering ESI was required to demonstrate that:

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.

---

[16] 241 F.R.D. at 545–46. Not all ESI is so difficult to authenticate. Requirements vary depending on the purpose for which the evidence is being offered. For example, certain courts have admitted ESI based on circumstantial evidence alone. 241 F.R.D. at 546 (citing various cases authenticating e-mail messages, transcripts of instant messaging conversations, and website postings based on such circumstantial evidence as the presence of an e-mail address, critical dates, or the substantive content).

[17] *See* 241 F.R.D. at 548–59.

[18] *See* Williams v. Sprint/United Management Co., 230 F.R.D. 640, 655, 62 Fed. R. Serv. 3d 1052, 29 A.L.R.6th 701 (D. Kan. 2005).

[19] Lorraine, 241 F.R.D. at 559.

[20] 241 F.R.D. at 534, 559.

[21] In re Vee Vinhnee, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005).

11. if the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.[22]

Although a given court may not impose such a rigorous standard, "[i]f 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."[23]

In *People v. Clevenstine*,[24] the defendant argued that a computer disk containing instant messages sent between himself and his alleged rape victims on MySpace had not been properly authenticated. The appellate court disagreed, citing "ample authentication for admission" of the evidence because:

[B]oth victims testified that they had engaged in instant messaging about sexual activities with defendant through the social networking site MySpace, an investigator from the computer crime unit of the State Police related that he had retrieved such conversations from the hard drive of the computer used by the victims, a legal compliance officer for MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by defendant and the victims, and defendant's wife recalled the sexually explicit conversations she viewed in defendant's MySpace account while on their computer.[25]

The court further found that the question of whether someone else had accessed the defendant's MySpace account was a factual issue for the jury to resolve.[26]

Moreover, *Palisades Collection, LLC v. Kedik*,[27] is an example of how some state courts are becoming more particular about authentication of ESI. In this case, Plaintiff offered the affidavit of its agent, which included printed copies of pages from an electronic spreadsheet as an exhibit. The appellate court affirmed the trial court's finding that the agent's affidavit testimony failed to establish "when, how, or by whom the electronic spreadsheet submitted in paper form was made," or "that the printed electronic spreadsheet submitted to the court was a true and

---

[22] In re Vee Vinhnee, 336 B.R. at 446.

[23] Lorraine, 241 F.R.D. at 559. *But see* U.S. v. Lubich, 72 M.J. 170 (C.A.A.F. 2013), in which the court, using the Military Rules of Evidence analog to the Federal Rules of Evidence, held that the court need not rely upon "the type of detailed analyses for the authentication of data set forth in *In re Vee Vinhee* and *Lorraine v. Markel*" because the court was satisfied that a *prima facie* showing of authenticity had been made to admit the evidence, and that further questions about the accuracy or other aspects of the character of the evidence went to weight, not admissibility and that "the defense had the opportunity to attack the perceived weaknesses in the case on cross examination." 72 M.J. at 171, 173. The court noted that while "there are numerous scenarios" in which the need to apply the *Vinhee* and *Lorraine* analysis will apply, it saw "no benefit in attempting to craft a 'standard' test to analyze all computer situations." 72 M.J. at 173.

[24] People v. Clevenstine, 68 A.D.3d 1448, 891 N.Y.S.2d 511 (3d Dep't 2009).

[25] Clevenstine, 891 N.Y.S.2d at 514.

[26] 891 N.Y.S.2d at 514.

[27] Palisades Collection, LLC v. Kedik, 67 A.D.3d 1329, 890 N.Y.S.2d 230 (4th Dep't 2009).

accurate representation of the record kept by the defendant."[28]

Some courts and litigants, however, place lesser emphasis on the unique authentication issues associated with ESI than may be indicated by the nature of that evidence. For example, the court in *Loyal v. State*, held that a "witness's lack of personal knowledge regarding how the records were created does not render them inadmissible, but merely affects the weight given to the evidence."[29] In that case, the plaintiff's vice president testified that the company maintained an electronic security log that recorded an employee's personal identification number (PIN) contemporaneously when the employee used the PIN to enter the warehouse. The court found this testimony sufficient to justify admission of a printed copy of the log under the business records exception to the hearsay rule, and never discussed the issue of authentication.[30]

16:6. Admissibility of evidence at trial—Hearsay

As noted above, issues of admissibility are not generally different for ESI than for paper evidence. However, the determination of whether proffered ESI evidence constitutes hearsay requires particular attention. Federal Rule of Evidence 801 defines hearsay as a "statement" made by a "declarant" that is offered "in evidence to prove the truth of the matter asserted."[1] A "statement" is defined as an act by a "person."[2] Similarly, a "declarant" is defined as "the person who made the statement."[3]

These definitions prove critical with respect to ESI. While a memorandum written by an individual using a computer may well constitute hearsay, many other common types of ESI are not necessarily hearsay. For instance, as explained by Judge Grimm, a report created by a fax machine is not hearsay.[4] First, there is no "person" involved in the creation of a "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received. Moreover, in this example, there is no "assertion" being made. For that reason, the record created by the fax machine is not a statement and cannot constitute hearsay.[5] This same rationale would apply to a wide variety of common computer-generated records, such as receipts automatically generated by a gasoline pump, or the information at the bottom of printout from an Internet web site identifying the source.

To be sure, assuring the accuracy of human testimony is different than assuring accuracy of computer-generated records. The accuracy of statements made by humans can be tested in the crucible of cross-examination if the unique circumstances surrounding the statements do not attest to their truth. The same cannot be said of computer-generated statements. It would be

---

[28] Palisades Collection, LLC, 890 N.Y.S.2d at 231.

[29] Loyal v. State, 300 Ga. App. 65, 67, 684 S.E.2d 124, 126 (2009) (quoting Hamilton v. State, 297 Ga. App. 47, 48–49, 676 S.E.2d 773 (2009)).

[30] Loyal, 684 S.E.2d at 126.

[1] Fed. R. Evid. 801(c).

[2] Fed. R. Evid. 801(a).

[3] Fed. R. Evid. 801(b).

[4] Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 542, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).

[5] Lorraine, 241 F.R.D. at 542. *See also* U.S. v. Khorozian, 333 F.3d 498, 506, 61 Fed. R. Evid. Serv. 980 (3d Cir. 2003), as amended, (Aug. 25, 2003).

impossible to cross-examine the computer or the program used to generate the information contained in the proffered evidence. Rather, the accuracy of the information printed by a computer "should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy."[6] As such, accuracy of computer records is an issue of authentication, not hearsay.

Yet, the proffered email evidence must meet the business records exception requirement that it be created in the regular course of the entity's business, and that it is the regular course of the entity's business to create email. The failure to meet these requirements led to the exclusion of certain emails in *Deep Oil Spill By The Oil Rig "Deepwater Horizon" In the Gulf Of Mexico On April 20, 2012*. The court excluded two emails on the ground that they did not fit into any known hearsay exception, and explicitly noted that the proponent had failed to offer any proof as to a third email that it "was not sent or received casually, or that its creation was not an isolated incident."[7]

16:7. Admissibility of evidence at trial—Original writing rule

To be admissible, ESI must also satisfy the original writing rule. Federal Rule of Evidence 1002, commonly referred to as the "best evidence rule," states that "[a]n original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise."[1] In other words, an original writing is required where the contents of the writing are in question, but not "to prov[e] events that just happen to have been recorded or photographed, or those which can be proved by eyewitnesses ...."[2]

In *Lorraine*, Judge Grimm goes on to explain:

Whether the content is at issue is determined on a case-by-case basis. 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 are no witnesses available to testify, the rule would apply to the video recording.[3]

Thus, where parties seek to introduce ESI "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

---

[6] State v. Hall, 976 S.W.2d 121, 147 (Tenn. 1998). *See also* State v. Dunn, 7 S.W.3d 427, 432 (Mo. Ct. App. W.D. 1999) (holding that the admissibility of computer-generated telephone records "should be determined on the reliability and accuracy of the process involved").

[7] In re Oil Spill by the Oil Rig Deepwater Horizon in the Gulf of Mexico, on April 20, 2010, 87 Fed. R. Evid. Serv. 492 (E.D. La. 2012) (citing Imperial Trading Co., Inc. v. Travelers Property Cas. Co. of America, 2009 WL 2382787, *3 (E.D. La. 2009)).

[1] Fed. R. Evid. 1002.

[2] Lorraine, 241 F.R.D. at 576.

[3] 241 F.R.D. at 578–79.

of the permitted forms of secondary evidence is admissible."[4] These determinations are made in accordance with Federal Rules of Evidence 1001 to 1008, each of which has potential ramifications for the admissibility of ESI.[5]

Definitional Issues

Federal Rule of Evidence 1001 contains the definitions that underlie the original writing rule. Specifically, Federal Rule of Evidence 1001(a) states that "writings" include "letters, words, numbers, or their equivalent set down in any form."[6] Moreover, with regard to ESI, F.R.E. 1001(d) defines original as "any printout—or other output readable by sight—if it accurately reflects the information." Importantly, when 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 F.R.E. 1001."[7] This language is particularly helpful to companies that routinely transfer written information, such as warranty registration or claims information, to a computer database and retain only the latter. However, it is important that the computer record accurately reflect all of the information contained in the original written record, or the computer record may not be admissible as an original.[8]

Finally, F.R.E. 1001(e) defines a "duplicate" as "a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original."[9] To be sure, "[a] duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances

---

[4] 241 F.R.D. at 583 (Parties offer testimonial evidence to establish relevant facts. Expert witnesses regularly testify based on the content of writings with no need for admission of the writing relied upon. (Fed. R. Evid. 703). However, on occasion, a particular fact can only be proven by reference to a document, such as where there are no eyewitnesses to an event, or it is the document itself, such as a contract, will, or deed that is at issue, and it is in this case that the original writing rule comes into play. 241 F.R.D. at 578–79. *See also* Fed. R. Evid. 1002, Advisory Committee's Notes.)

[5] 241 F.R.D. at 576–77.

[6] Fed. R. Evid. 1001(1).

[7] 241 F.R.D. at 578 (citing In re Gulph Woods Corp., 82 B.R. 373, 377, 24 Fed. R. Evid. Serv. 891 (Bankr. E.D. Pa. 1988), in which the court held that "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").

[8] The court in *Gulph Woods* cautioned 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." 82 B.R. at 377 (citations omitted).

[9] Fed. R. Evid. 1001(e).

make it unfair to admit the duplicate."[10] This is important because ESI is commonly and often necessarily copied or duplicated to create a version that can be submitted as evidence. Therefore, the definition of "duplicate" may be critical to the introduction of certain types of ESI. For example, it may be difficult or even impossible to produce an original database for use at trial, whereas a copy of the database, or of information contained within the database, may well be a sufficiently duplicated and therefore admissible.

Secondary Evidence

In certain circumstances, secondary evidence may be used in place of an original writing. ESI is notoriously ephemeral and can easily be lost or destroyed, sometimes without any human intervention at all "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) ..."[11] Where this is the case "the only available proof of such information would be secondary evidence such as testimonial or other evidence."[12]

Crucially, F.R.E.1004 describes four circumstances in which secondary evidence is admissible in lieu of an original. These four circumstances are "(a) all the originals are lost or destroyed, and not by the proponent acting in bad faith;[13] (b) an original cannot be obtained by any available judicial process; (c) the party against whom the original would be offered had control of the original; was at that time put on notice, by pleadings or otherwise, that the original would be a subject of proof at the trial or hearing; and fails to produce it at the trial or hearing; or (d) the writing, recording, or photograph is not closely related to a controlling issue."[14] Notably, Judge Grimm illustrates the "collateral issue" exception as follows:

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.[15]

Yet, caution is advised when attempting to utilize secondary evidence concerning ESI. In *United States v. Bennett,* the trial court excluded testimony concerning GPS data on a ship allegedly smuggling narcotics, holding that the best evidence of that information would have been a screen shot, printout or other computer-generated documents or data, rather than the

---

[10] Fed. R. Evid. 1003.

[11] Lorraine, 241 F.R.D. at 580.

[12] 241 F.R.D. at 580.

[13] *See* 241 F.R.D. at 580 (citing People v. Huehn, 53 P.3d 733, 738 (Colo. App. 2002)). *See also* Fed. R. Civ. P. 37(e) (allowing a court to impose sanctions where the failure to produce ESI was not the result of the "routine, good faith operation of an electronic information system").

[14] Fed. R. Evid. 1004.

[15] Lorraine, 241 F.R.D. at 580.

testimony of a witness who viewed the GPS information.[16] To be sure, though, Federal Rule of Evidence 1004 may, in appropriate circumstances, be useful where ESI is lost or deleted because it allows a party to use secondary evidence to establish the contents of an original writing.

Summaries of Voluminous Evidence

Federal Rule of Evidence 1006 defines a special form of secondary evidence, allowing proof of voluminous records through summaries. This is particularly important and helpful for counsel as many forms of ESI are voluminous. For example, the only practical way for companies to introduce evidence of voluminous data contained in databases is a database report, which some courts have held to constitute a summary.[17]

Importantly, F.R.E. 1006 includes two caveats. First, summaries are admissible as evidence only when the "originals, or duplicates, [are] made available for examination or copying, or both, by other parties at a reasonable time and place,"[18] regardless of whether or not the originals were the subject of a formal request for production.[19] The second caveat is that the underlying voluminous information must be independently admissible.[20] Therefore, although F.R.E. 1006 provides for the admissibility of summaries, it does so at significant cost.

Authentication by Testimony of Party Opponent

The party opponent may also authenticate ESI. Specifically, Federal Rule of Evidence 1007 allows proof of the contents of writings, recordings, and photographs by "the testimony, deposition, or written statement of the party against whom the evidence is offered."[21] The evidence proffered through this method is admissible regardless of whether the original is available or not.[22]

Although rarely relied upon, F.R.E. 1007 can be a critically important method of proving the content of ESI. Given the volatile nature of ESI, the only evidence of an e-mail, word processing document, or some other type of ESI is often the recollection of a witness who

---

[16] U.S. v. Bennett, 363 F.3d 947, 64 Fed. R. Evid. Serv. 467 (9th Cir. 2004).

[17] U.S. v. Nixon, 694 F.3d 623, 89 Fed. R. Evid. Serv. 480 (6th Cir. 2012); In re Diet Drugs (Phentermine/Fenfluramine/Dexfenfluramine) Products Liability Litigation, 90 Fed. Appx. 643 (3d Cir. 2004). The rule has also been interpreted to allow admission of summaries in either written or testimonial form. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 581, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007) (citing Weinstein at §1006.05[2]). See also references to database evidence, *infra.*

[18] Fed. R. Evid. 1006. The rule further provides that the court may order that the originals or duplicates be produced in court.

[19] Lorraine, 241 F.R.D.at 581 ("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.") (quoting Weinstein at §1006.06[1]).

[20] 241 F.R.D. at 581.

[21] Fed. R. Evid. 1007.

[22] Lorraine, 241 F.R.D. at 582.

created, read, or dealt with the information. In this situation, if the testimony of the person with knowledge of the ESI in question would qualify as an admission under Fed. R. Evid. 801(d)(2), then his or her testimony is admissible under F.R.E. 1007 to prove the contents of the ESI.[23]

Conditional Relevance

Federal Rule of Evidence 1008 "allocates responsibility between the trial judge and the jury with respect to certain preliminary matters affecting the original writing rule."[24] F.R.E. 1008 is, in fact, a special application of the conditional relevance rule, Rule 104.[25] Generally, the court is empowered to decide issues like whether an original document has been lost for purposes of F.R.E. 1004 or whether records are "voluminous" for purposes of Rule 1006.[26] However, F.R.E. 1008 identifies three determinations that fall to the jury. Specifically, where "an issue is raised (a) whether the asserted writing, recording or photograph ever existed, or (b) whether another one produced at the trial or hearing is the original, or (c) whether other evidence of content accurately reflects the content."[27]

Federal Rule of Evidence 1008 can be significant in the context of ESI. For example, where the original has been lost or destroyed, a dispute might arise about whether secondary evidence offered in lieu of the original accurately reflects the contents of the original record. Similarly, because of the ease with which this ESI can be altered, intentionally or otherwise, disputes may arise about different versions of the same record that are offered into evidence. In these cases, the jury must decide the questions of fact that are raised.

16:8. Admissibility of evidence at trial—Specific evidence types

Certain types of ESI not only commonly appear in modern litigation, but also pose unique challenges in terms of trial preparation. Among these are e-mail, web page content, information contained in databases, and videos. Admissibility issues with regard to each type are discussed below.

E-mail

Perhaps the most important and commonly used type of ESI is email. Indeed, given its widespread use, virtually all litigants have an expectation that e-mail will be produced in discovery in any matter involving issues arising in the last decade.[1] Moreover, as the primary form of written communication both within and outside businesses, e-mail is a likely repository

---

[23] 241 F.R.D. at 582 (citing Weinstein at §§1007.03[1], 1007.06). Responses to requests for admission or interrogatories are similarly admissible under Rule 1007. 241 F.R.D. at 582.

[24] 241 F.R.D. at 582.

[25] Fed. R. Evid. 1008, Advisory Committee's Notes.

[26] Fed. R. Evid. 1008, Advisory Committee's Notes.

[27] Fed. R. Evid. 1008.

[1] *See, e.g.*, Email Statistics Report, 2014–2018—Executive Summary-April 2014, The Radicati Group, Inc, http://www.radicati.com. In 2015, the average corporate user is predicted to send about 116 e-mail messages per day, with continued expected growth every year.

for relevant information.[2] This is true, in part, because e-mail messages tend to propagate further, and live longer, than other forms of ESI. Further, e-mail messages often contain attachments of documents that have not been downloaded to a computer and therefore may not exist anywhere else. Thus, in light of the fact that e-mail will almost certainly be part of any litigation, a party must ensure that all foundational requirements for admissibility are understood.

A number of courts have addressed evidentiary issues involving e-mail. The admissibility of emails depends largely on the perceived importance of the evidence. In the oft-cited case of *Fenje v. Feld*, the court held that "[e]-mail communications may be authenticated as being from the purported author based on an affidavit of the recipient; the e-mail address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the e-mail communication that is being authenticated."[3] Thus, courts have found that an e-mail message may be authenticated by showing that the email was produced from the opposing party's files and that the text of the email indicates that it was sent by the opposing party.[4] Similarly, the testimony of a witness who either sent or received an e-mail message will be sufficient to authenticate an e-mail message.[5]

Yet courts have cautioned against foundational complacency, warning that email will not be admitted merely on a foundation that the sender or recipient regularly sends or receives email. These courts have, to a great extent, required strict adherence to standard business practices foundations to meet an element of trustworthiness of the email offered as evidence. The Fourth Circuit noted in *United States v. Cone* that "it would be insufficient to survive a hearsay challenge simply to say that since a business keeps and receives emails, then *ergo* all those emails are business records falling within the ambit of Rule 803(6)(B)."[6] The Eastern District of Pennsylvania in *Roberts Technology Group v. Curwood, Inc.,* sounded a warning that is blunt but eloquent in its simplicity; the court wrote that while there of course is no blanket rule excluding email as a business record, the opposite is true and there is no "absolute right to admission of emails under the business records exception." The party offering the emails must "provide

---

[2] *See, e.g.,* U.S. v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) ("[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").

[3] Fenje v. Feld, 301 F. Supp. 2d 781, 809, 185 Ed. Law Rep. 609 (N.D. Ill. 2003), aff'd, 398 F.3d 620, 195 Ed. Law Rep. 469 (7th Cir. 2005). *See also* U.S. v. Safavian, 435 F. Supp. 2d 36, 40 n.2 (D.D.C. 2006) (indicating that e-mail messages can be authenticated by a witness with personal knowledge that the message is what it is claimed to be); Guang Dong Light Headgear Factory Co., Ltd. v. ACI Intern., Inc., 2008 WL 53665 (D. Kan. 2008) (e-mail message authenticated by affidavit of custodian).

[4] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 971–72 (C.D. Cal. 2006). *See also* In re Homestore.com, Inc. Securities Litigation, 347 F. Supp. 2d 769, 781 (C.D. Cal. 2004) (e-mails deemed authentic because they were produced by the objecting party).

[5] *See, e.g.,* Tibbetts v. RadioShack Corp, 10 Wage & Hour Cas. 2d (BNA) 148, 2004 WL 2203418, *13 (N.D. Ill. 2004) (finding that a witness' testimony that proffered e-mail are "true and correct copies of his own correspondence" sufficiently authenticated the records).

[6] U.S. v. Cone, 714 F.3d 197, 91 Fed. R. Evid. Serv. 149 (4th Cir. 2013); Brown v. West Corp., 2014 WL 1794870, *3 (D. Neb. 2014).

specific foundational evidence allowing the Court to find the statements trustworthy." The court declined to admit the proffered emails because there was no evidence offered that the emails were regular business records, had been received consistent with regular business practices or had been retained pursuant to an email or electronic data policy.[7]

Parties can authenticate e-mail messages based on technological considerations that are independent of the source of production and content of the email. At least one court has recognized that the Internet Protocol address in an e-mail message header is a means by which the sender can be identified.[8] Another court held that an e-mail address alone constitutes a mark of origin sufficient to self-authenticate an e-mail message under F.R.E. 902(7).[9] Significantly, in *E.E.O.C. v. Olsten Staffing Servs.,* the court rejected the argument that "only the *author* of the e-mails may authenticate them," because, under such a rule, "e-mails would be inadmissible in any case in which the purported author denied their accuracy."[10] Instead, the court opined that "[t]estimony from someone who personally retrieved the e-mail from the computer to which the e-mail was allegedly sent is sufficient" to support a finding that the e-mail is that which the proponent claims.[11]

On the other hand, courts have readily refused to admit e-mail messages where the party proffering the evidence offered insufficient foundation. For instance, courts have refused to admit e-mail as evidence where the content of the message is factually incorrect or inconsistent with the authenticating testimony.[12] Also, in *Eastview Healthcare, LLC v. Synertx, Inc.*, the court rejected the argument that e-mails were authenticated by virtue of having been produced in discovery under the prevailing rule that "'[u]pon production of copies pursuant to a notice to produce, the producing party admits the correctness of the copies and further proof is

---

[7] Roberts Technology Group, Inc. v. Curwood, Inc., 2016 WL 2889166, *2 (E.D. Pa. 2016). *See also* Candy Craft Creations, LLC v. Gartner, 2015 WL 6680883, *2-3 (S.D. Ga. 2015), holding that all persons in the email chain must be acting within the regular course of business—otherwise, "an essential link in the trustworthiness chain is missing." The court also noted that the failure to establish that all pertinent parties to the emails were acting within the scope of regularly conducted business practices adversely affected the reliability of the emails as evidence.

[8] Clement v. California Dept. of Corrections, 220 F. Supp. 2d 1098, 1111 (N.D. Cal. 2002), aff'd, 364 F.3d 1148 (9th Cir. 2004) ("The evidence in the record suggests that Internet-produced materials are, in fact, easier to trace than anonymous letters because the major e-mail providers include a coded Internet Protocol address (IP address) in the header of every e-mail. The IP address allows the recipient of an e-mail to identify the sender by contacting the service provider.") (citations to record omitted).

[9] Superhighway Consulting, Inc. v. Techwave, Inc., 1999 WL 1044870, *2 (N.D. Ill. 1999).

[10] U.S. E.E.O.C. v. Olsten Staffing Services Corp., 657 F. Supp. 2d 1029, 1034 (W.D. Wis. 2009).

[11] Olsten Staffing Services Corp., 657 F. Supp. 2d at 1034.

[12] Network Alliance Group, LLC. v. Cable & Wireless USA, Inc., 2002 WL 1205734, *1 (D. Minn. 2002) (noting that "date stamp" on e-mail proffered in support of request for injunction reflected a future date and an incorrect day of the week).

unnecessary in order for the moving party to introduce them into evidence.'"[13] The court instead held that the rule as such only applies to documents produced by the opposing party and that parties must authenticate the documents they produce in discovery on their own.[14]

Admissibility of email may also figure prominently in dispositive motions, which may require support by proof in admissible form. In *Lorraine v Markel American Insurance Co.,* both parties filed summary judgment motions with printouts of emails as exhibits, but neither party provided any basis for authentication of those printouts. In a lengthy opinion that discussed the spectrum of foundation requirements for ESI, and email in particular, Judge Grimm denied both motions, largely upon the inadmissibility of the email printouts.[15] Similarly, the court in *Bowers v. Rector and Visitors of the University of Virginia* the court was faced with a motion that contained over 600 pages of email printouts. Counsel's attempt at authentication comprised her own affidavit stating that the emails were received from her adversary in discovery. The court denied the motion, and in doing so served a rather stern warning to the bar concerning the need for a proper foundation when appending evidence in support of a dispositive motion:

[T]he submission by plaintiff's counsel of ... more than fifty unauthenticated copies of e-mails convincingly demonstrates both a recklessness and an absence of preparation on the part of plaintiff's counsel. Equally so, her resort to use of her own affidavit in a misguided quick-and-easy attempt to fix significant evidentiary deficiencies, demonstrates a recklessness in preparation and a failure to exercise legal judgment abject.[16]

Web Page Contents

Web page content can be extremely useful in modern litigation against both corporate and individual litigants. Although locating relevant information is relatively easy, admitting web pages into evidence at trial is difficult. Importantly, the courts generally agree that "[p]rintouts from a web site do not bear the indicia of reliability demanded for other self-authenticating documents under Fed. R. Evid. 902."[17] This is because "[a]nyone may purchase an Internet

---

[13] Eastview Healthcare, LLC v. Synertx, Inc., 296 Ga. App. 393, 397, 674 S.E.2d 641, 645 (2009) (quoting Willis v. Hill, 116 Ga. App. 848, 159 S.E.2d 145 (1967), judgment rev'd on other grounds, 224 Ga. 263, 161 S.E.2d 281 (1968)).

[14] Eastview Healthcare, LLC, 296 Ga. App. at 397, 674 S.E.2d at 646.

[15] Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).

[16] Bowers v. Rector and Visitors of University of Va., 2007 WL 2963818, *1 (W.D. Va. 2007), on reconsideration in part, 2008 WL 2346033 (W.D. Va. 2008).

[17] In re Homestore.com, Inc. Securities Litigation, 347 F. Supp. 2d 769, 782 (C.D. Cal. 2004) (holding that press and earnings releases printed from the defendant's web site were inadmissible for purposes of summary judgment motion absent authenticating affidavit or other evidence by someone with personal knowledge of the accuracy of the information); *cf* U.S. v. Hassan, 742 F.3d 104, 132–33, 93 Fed. R. Evid. Serv. 758 (4th Cir. 2014), cert. denied, 134 S. Ct. 2737 (2014) and petition for certiorari filed, 2014 WL 2880987 (U.S. 2014) (holding that the trial court did not abuse its discretion by holding that Facebook pages and YouTube videos were self-authenticating under 902(11) as business records where the evidence was supported by

address, and so, without proceeding to discovery or some other means of authentication, it is premature to assume that a webpage is owned by a company merely because its trade name appears in the [url]."[18] Therefore, counsel must provide a sufficient foundation for the web page before it is entered into evidence.

Printouts of webpages can be authenticated a number of ways. First, a party can use circumstantial evidence. For instance, in *Tienda v. State*, the court admitted a printout of the defendant's Myspace page into evidence where "internal content"—photographs, music, and comments on the page that were distinct to one party—was sufficient to lead a reasonable juror to believe that the Myspace page was created by the defendant.[19] Second, a party can obtain the information necessary to authenticate the Web site "through an interrogatory, request for admission, or a deposition of a party with knowledge of the website."[20] Indeed, in in *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, printouts of a website obtained from the Internet Archive were admitted into evidence based on an affidavit of a representative of the Internet Archive stating that it had "retrieved copies of the website as it appeared on the dates in question from its electronic archives."[21] Noting that the plaintiff had offered "no evidence that the Internet Archive is unreliable or biased," and had "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," the court held that the affidavit was "sufficient to satisfy Rule 901's threshold requirement for admissibility."[22] However, an attorney's declaration as an officer of the court that the printout is a "true and correct copies of web pages from [the defendant's] website"

---

certifications of records custodians at Facebook and Google that the pages and videos were kept as business records.).

[18] Victaulic Co. v. Tieman, 499 F.3d 227, 236, (3d Cir. 2007), as amended, (Nov. 20, 2007) (holding that trial court improperly took judicial notice of facts contained on plaintiff's Internet web site in part because the evidence was not properly authenticated). The court also noted that corporate web pages are marketing tools "full of imprecise puffery that no one should take at face value." Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007), as amended, (Nov. 20, 2007). The same would surely hold true about Internet web pages purportedly identifying an individual rather than a corporation, and the information contained thereon.

[19] Tienda v. State, 358 S.W.3d 633, 642 (Tex. Crim. App. 2012).

[20] Kohler v. Kindred Nursing Centers West, LLC, 2010 WL 709182, *6 (Cal. App. 4th Dist. 2010), unpublished/noncitable.

[21] Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 65 Fed. R. Evid. Serv. 673, 2004 WL 2367740, *1 (N.D. Ill. 2004).

[22] Telewizja Polska USA, Inc., 2004 WL 2367740, *6. The court also rejected the plaintiff's hearsay objections, finding that, "'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.'" 2004 WL 2367740, *5 (quoting Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002)). Furthermore, "the contents of [a] website may be considered an admission of a party-opponent, and are not barred by the hearsay rule." 2004 WL 2367740, *5.

is not sufficient.[23]

Importantly, the purpose for which the evidence is being proffered influences the admissibility of a website printout. Specifically, in *Saadi v. Maroun*, testimony from the plaintiff that he "personally saw the postings and printed them off his computer" was sufficient to admit the printouts into evidence in a defamation case.[24] The court emphasized, however, that the plaintiff had offered the printouts for the "limited purpose of proving that the statements appeared on the world wide web," and that the printouts would have had to have been authenticated "by calling a website owner or webmaster if Saadi had offered the postings to prove that the postings came from a specific person or organization."[25]

Database Content

Corporations rely increasingly on data contained in a variety of databases. Common examples include production data, financial information, and claims data. As a result, parties often need to proffer information originally housed in databases as evidence at trial or in support of dispositive motions. Indeed, there is no doubt that, as a general rule, information contained in electronic databases is discoverable.[26] Such data, however, poses particular challenges as it is generally difficult or impractical to offer the opposing party access to the databases themselves.

Although database extracts are commonly used in trial, few cases to date directly address the admissibility of database extracts as evidence. Nevertheless, the basic foundational principles discussed above apply to database extracts as well. That is to say that database extracts must be shown to be what they purport to be. For example, one court has identified a number of unique evidentiary questions that pertain to the admissibility of information stored in a computer database:

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.[27]

Parties may be tempted to offer database content under F.R.E. 1006 as a summary of voluminous records. Indeed, databases quite often contain voluminous information that "cannot

---

[23] Kohler, LLC, 2010 WL 709182, *5–6.

[24] Saadi v. Maroun, 2009 WL 3736121 (M.D. Fla. 2009).

[25] Saadi, 2009 WL 3736121, *4.

[26] *See, e.g.,* Bank One, N.A. v. Echo Acceptance Corp., 2006 WL 2564262 (S.D. Ohio 2006) (ruling that information contained in electronic databases that was not duplicative of hard copy document already produced was discoverable).

[27] In re Vee Vinhnee, 336 B.R. 437, 448 (B.A.P. 9th Cir. 2005) (excluding evidence of electronically stored business records that had not been properly authenticated).

conveniently be examined in court."[28] However, F.R.E. 1006 also provides that, where a party relies on a summary, the "proponent must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."[29] Thus, even making an offer of a database extract under F.R.E. 1006 may subject the company's database to examination by the opposing party, which would, in most cases, be an entirely unintended and undesirable consequence.

In any event, most database extracts are probably not summaries as contemplated by F.R.E. 1006. To be sure, rather than summarizing a larger body of information, most database extracts are actually unique subsets of data that are complete unto themselves. For example, a database extract of warranty claims for a specific product can hardly be considered a summary of all warranty claims for all products. Thus, rather than place the company's entire database at risk, a corporate defendant would be better served by preparing to authenticate database content as it would most other ESI: through the testimony of someone familiar with the database, the computer system on which it operates, and the methodology for entering and retrieving data. For instance, a trial court admitted a report from a database where the foundational testimony showed that the report was based on information entered into the database in the ordinary course of business, and the database was regularly maintained and updated by company accountants with personal knowledge of information in the database.[30] Indeed, the Sixth Circuit in *U.S. v. Nixon* held that a database summary that was printed in response to a subpoena was admissible as a business record under Federal Rule of Evidence 803(6).[31] Therefore, database content may be able to be admitted into evidence without subjecting the entire database to examination.

Video

Video evidence is also a useful form of ESI that has special admissibility considerations. For instance, in *People v. Roberts*, the appellate court explained that, "because films are so easily altered, there is a very real danger that deceptive tapes, inadequately authenticated, could contaminate the trial process," and therefore videotape evidence must be authenticated either by "the testimony of a participant or witness to the events, such as a videographer," or through a "chain of custody" method.[32] The latter method requires that "in addition to evidence concerning the making of the [video]tape [] and identification of the [participants], that within reasonable limits those who have handled the [video]tape from its making up to production in court 'identify it and testify to its custody and unchanged condition.'"[33] The court found that the trial court abused its discretion in admitting the videotape because "there was no testimony concerning the making of the videotape, where it was kept or who had access to it during the nearly three-year

---

[28] Fed. R. Evid. 1006.

[29] Fed. R. Evid. 1006.

[30] McClendon v. Challenge Financial Investors Corp., 2009 WL 589245 (N.D. Ohio 2009).

[31] U.S. v. Nixon, 694 F.3d 623, 634, 89 Fed. R. Evid. Serv. 480 (6th Cir. 2012); *see also* U.S. v. Moon, 513 F.3d 527, 75 Fed. R. Evid. Serv. 593 (6th Cir. 2008)

[32] People v. Roberts, 66 A.D.3d 1135, 887 N.Y.S.2d 326, 327–28 (3d Dep't 2009).

[33] Roberts, 887 N.Y.S.2d at 328 (modifications in original) (quoting People v. Ely, 68 N.Y.2d 520, 527, 528, 510 N.Y.S.2d 532, 503 N.E.2d 88 (1986)) (citations omitted).

period from the time of its making to its discovery."[34] In granting the defendant's request for a new trial, the court observed that the prosecution would have the "opportunity to remedy the foundational deficiencies" by, for example, providing an expert witness to testify that the tape "fairly and accurately depicted what was before the camera and that an analysis of it revealed no indication of alterations."[35]

Moreover, in *State v. Berke*, the Supreme Judicial Court of Maine demonstrated that the modicum of evidence required to establish authenticity by chain of custody is not great.[36] In this case, the prosecution offered in evidence several videotapes seized from the defendant's home, as well as a videotape allegedly copied from his video camera by the sister of one of the victims.[37] Applying a standard "identical to that set forth in [Rule 901 (b) of] the Federal Rules of Evidence," the court held that the lower court's "findings regarding [the defendant's] continual presence in the tapes and the largely sequential nature of the events depicted in the tapes support an inference that the tapes had not been altered and that they are what the proponent ... claimed them to be[.]"[38]

Non-U.S. ESI

Electronic evidence that originates outside the United States or resides in repositories outside U.S. borders may pose specific evidentiary challenges. These include authentication in the absence of the availability of live testimony, the business records exception to the Hearsay Rule, and admissibility of such non-email ESI as database reports, text messages, social media posts, and Internet cache files.[39]

The challenges in overcoming the business records exception for email and other communications that originate beyond the U.S. may be particularly daunting because evidence to support the proposition that the email was created in the regular course of business may not be readily available. Meeting the tenet of the business records exception may be met by a showing that the information was maintained as required by local law that mandates safeguards for that

---

[34] 887 N.Y.S.2d at 328.

[35] 887 N.Y.S.2d at 329. *See also* People v. Taylor, 398 Ill. App. 3d 74, 337 Ill. Dec. 658, 922 N.E.2d 1235 (2d Dist. 2010), judgment rev'd, 2011 IL 110067, 353 Ill. Dec. 569, 956 N.E.2d 431 (Ill. 2011) (holding that trial court erred in admitting videotape where "the evidence plainly shows that the device was not operating properly; that there was no preservation of the original recording; that there was no proper chain of custody; and that an unexplained copying took place"; however, on review, the Supreme Court held that in a matter of first impression, the state had, in fact, laid a proper foundation for admission of the surveillance videotape and, in so doing, the Supreme Court disagreed with certain of the appellate court's factual conclusions and also held that the appellate court had taken an unduly restrictive view of the pertinent foundational requirements.).

[36] State v. Berke, 2010 ME 34, 992 A.2d 1290 (Me. 2010).

[37] Berke, 2010 ME 34, 992 A.2d at 1291–92.

[38] 2010 ME 34, 992 A.2d at 1292–93.

[39] Rashbaum, Knouff and Murray, Admissibility of Non-U.S. Electronic Evidence, XVIII Rich. J. L. & Tech. 9 (2012), http://jolt.richmond.edu/v18i3/article9.pdf

information.[40] Rules for self-authentication, such as F.R.E. 902(7), which states that the record may be self-authenticated if it bears "[A]n inscription, sign, tag or label purporting to have been affixed in the course of business and indicating origin, ownership, or control," may be of great assistance in establishing foundation for admissibility. This standard may, arguably, be met by the appearance of a corporate signature block on a company's email, though Judge Grimm has cautioned that this Rule has not been used in this innovative way with great frequency.[41] Other means of self-authentication may include F.R.E. 902(12) which has proved to be an efficient path to admission, for at least certain types of ESI. Specifically, F.R.E. 902(12) concerns "Certified Foreign Records of a Regularly Conducted Activity."109 By reference to F.R.E. 902(11), this provision requires that the evidence be admissible under F.R.E. 803(6)(A) to (C) (a business records exception for "Records of Regularly Conducted Activity"), *if* accompanied by a declaration certifying:

> (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
>
> (B) the record was kept in the course of a regularly conducted activity of a business ...; and
>
> (C) making the record was a regular practice of that activity.[42]

Many courts will opt for a lower bar on authentication of non-U.S. documents, preferring to permit the jury to allot such weight to the records as it sees fit, if the documents have sufficient indicia of reliability. In this way, pursuant to F.R.E., courts have admitted medical records from Guatemala[43] and shipping documents from the U.K.[44] without the certifications required by the Federal Rules of Evidence.

16:9. Conclusion

Extraordinary resources have gone into educating the bench and the bar about the discovery of electronically stored information. However, discovery of such information will be to no avail if it cannot be offered as evidence at trial. In the past, decisions about establishing the proper foundation for the admissibility of evidence could safely be deferred until trial was imminent. Today, because ESI can be altered so as to make it inadmissible simply through the collection process, corporate litigants and their counsel must begin thinking about these issues much earlier. Therefore, counsel must be aware of the methods of admitting varying types of ESI into evidence, and the consequences of both ESI destruction and failing to timely object to the proffer of ESI.

---

[40] XVIII Rich. J. L. & Tech. at 18.

[41] Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 537–38, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007). *See generally* Grimm et al., Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information, 42 Akron L. Rev. 357, 389 (2009); Rashbaum, Knouff, and Murray, "Admissibility of Non-U.S. Electronic Evidence," XVIII Rich. J. L. & Tech. 9 (2012), http://jolt.richmond.edu/v18i3/article9.pdf, at 27, n. 108.

[42] XVIII Rich. J. L. & Tech. 9 (2012), http://jolt.richmond.edu/v18i3/article9.pdf, at 27, n. 108., and citation therein.

[43] *See* Escriba v. Foster Poultry Farms, 793 F. Supp. 2d 1147, 1156–57 (E.D. Cal. 2011).

[44] *See* U.S. v. Parker, 749 F.2d 628, 633, 17 Fed. R. Evid. Serv. 1364 (11th Cir. 1984).