Admissibility of Electronically Stored Information: It's Still the Same Old Story*

by
Sheldon M. Finkelstein** and
Evelyn R. Storch***

As time goes by, the proliferation of electronic documents means that lawyers will continue to face ever rising mountains of electronically stored information ("ESI"). The sheer quantity of information and the often unintelligible forms it can take present formidable challenges to lawyers who want to turn that material into admissible evidence.[1] This article will address those challenges and provide practical guidance on how to meet them.

The authors assume you are diligent regarding ESI. You know the rules and you follow them. Your client has been preserving its ESI and is producing what is required of it, and you are wringing every last bit of ESI out of your adversary. You expect to obtain some excellent information in the discovery process that you definitely will want to use at trial. You've been thinking about the evidence you're collecting and checking it against the theme you have created for the case. So what now? How do the evidence rules, written in a time of paper documents and tangible things, apply? How do you get your ESI into evi-

---

* This article is adapted from and expands significantly upon one that first appeared in *Litigation*, published by the American Bar Association, in May 2008. Scattered throughout this article are lyrics taken from the song, *As Time Goes By*, written by Herman Hupfeld in 1931 and popularized in the movie, *Casablanca*.

** Podvey, Meanor, Catenacci, Hildner, Cocoziello & Chattman, A Professional Corporation, Newark, New Jersey. The authors wish to acknowledge the assistance of Elana Bensoul, a summer intern with Podvey Meanor and a law student at Columbia Law School (Class of 2011), in the research of this article.

*** Counsel, Harwood Lloyd, LLC in Hackensack, NJ.

1 *See e.g.,* David Narkiewicz, *Where to Look for Electronically Stored Information*, 52 PA. LAW. 52 (Mar./Apr. 2009).

dence at the time of trial? How can you keep your adversary's out?

The Fundamental Things Apply

Despite all the technological advances, when it comes to admissibility of ESI, you must start with the basics: Is the evidence relevant? Can I authenticate it (and are there special authentication problems associated with ESI)? Will I have a hearsay problem? Is the form of the ESI considered an original or is there secondary evidence to prove its content? Is it so prejudicial that it would be unfair to admit it? These questions are well known to you. Indeed, the issues of relevance and prejudice have few problems unique to ESI and, therefore, will not be discussed in this article except as they might intersect the issues addressed here. On the other hand, answers to the questions regarding authenticity, hearsay and the "original document rule," as they pertain to ESI, have proven to be elusive.

With little controlling authority and a variety of judicial approaches, you must be prepared to meet the most rigorous standards. After a time, when more judges will have been raised on computers, the suspicion in several judicial quarters surrounding the creation and potential alteration of ESI may diminish, and the requirements for admissibility may be less demanding. But, for now, there remain substantial pockets of judicial skepticism which result, in some courts, in exacting foundational requirements you must be prepared to satisfy.

That No One Can Deny

Trial attorneys often take authentication for granted. It seems simple enough. You merely have to provide "evidence sufficient to support a finding that the matter in question is what its proponent claims."[2] ESI, however, can require scientific proof of your computer processes. Absent prior thorough analysis, you may lose the right to discharge that smoking gun e-mail you thought would be the linchpin of your case.

A helpful starting place for any analysis of admissibility of ESI is Chief United States Magistrate Judge Paul W. Grimm's

---

[2] FED. R. EVID. 901.

decision in *Lorraine v. Markel American Ins. Co.*[3] The lengthy "soup to nuts" opinion is an authority-rich discourse of every facet of the admission of evidence generally and of ESI in particular.

Judge Grimm instructs that, before you can determine how you will authenticate your ESI, you first must consider the interplay of Federal Rules of Evidence 104(a) and (b).[4] Under subsection (a), the judge determines preliminary questions concerning the admissibility of evidence and, in that determination, is not bound by the rules of evidence.[5] Subsection (b), on the other hand, requires that the jury determine relevance if it is based on fulfillment of a condition of a fact.[6] Authenticity of evidence falls under subsection (b), because the relevance is conditioned upon its being what it purports to be. By way of example, the authenticity of a web page must be decided by a jury, and the foundation must be laid with admissible evidence. Whether that web page is (or contains) hearsay, on the other hand, will be judicially determined upon a foundation that may or may not itself be admissible.

To authenticate evidence, as required by Federal Rule of Evidence 901(a), you need only make a prima facie showing that the ESI is what it purports to be. Some courts will require rigorous proofs that the computer processing system is reliable and its output is accurate.[7] Others will permit ESI into evidence upon the testimony of a person with knowledge who explains the system's operation and identifies the record as having been produced by the system.[8] Authentication of ESI is, in short, decided on a case by case basis upon standards that may vary from juris-

---

3 241 F.R.D. 534 (D. Md. 2007). Another excellent source is the Program Material for the August 2007 ABA Annual Meeting: Linda L. Listrom, Eric R. Harlan, Elizabeth H. Ferguson and Robert M. Redis, *The Next Frontier: Admissibility of Electronic Evidence,* available at http://www.abanet.org/abanet/common/login/securedarea.cfm?areaType=premium&role=lt&url=/Litigation/mo/premium-lt/prog_materials/2007_abaannual/27.pdf (last visited September 20, 2009).

4 241 F.R.D. at 539.

5 FED. R. EVID. 104(a).

6 FED. R. EVID. 104(b).

7 *In re Vee Vinhnee*. 336 B.R. 437, 448 (9th Cir. 2005).

8 *E.g., State v. Sanders.,* 2007 WL 5290431, *3 (AZ Ct. App. Dec. 24, 2007).

diction to jurisdiction and even from jurist to jurist.[9] As a result, there is substantial room for creativity by you as both the proponent and the opponent of evidence.

Although Rule 901(a) does not specify how to authenticate evidence, Rule 901(b) provides ten non-exclusive illustrations.[10] Subsections (1), (3), (4), (7), and (9), with particular emphasis on subsections (4) and (7), have relevance to ESI. You can authenticate ESI under Rule 901(b)(1) through the testimony of a witness with knowledge. The creator qualifies, but anyone with knowledge is sufficient. In the case of ESI, the authenticating witness must be able to establish not only its creation but its preservation without alteration. Authentication by comparison with other authenticated specimens under Rule 901(b)(3) can be useful for ESI, especially e-mails, and one court has already permitted this form of authentication.[11] For example, an e-mail with no identifying information and a screen name bearing no relationship to a person's name (such as moviebuff1942@worldcom.com) can be authenticated by an e-mail already in evidence that bears the same characteristics as the e-mail to be authenticated and in which moviebuff1942 identifies herself. Rule 901(b)(9) was designed with computer information in mind and is self-explanatory. It permits authentication by "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."[12] Most companies' "techies" will have little trouble authenticating ESI in this manner.

The rule most frequently used for ESI, particularly e-mails, is Federal Rule of Evidence 901(b)(4). That rule permits authentication by "distinctive characteristics," including the substance of the evidence. In our example above, the comparison e-mail from moviebuff1942@worldcom.com, itself, might have been authenticated under this rule by the presence of both the sender's screen and real name, its contents, and corroboration linking the

---

9 There is also some variation depending on the format. *See* Kevin F. Brady et al., *The Sedona Conference Commentary on ESI Evidence & Admissibility*, 9 SEDONA CONF. J. 217, 222 (2008) (discussing authentication of web postings, text messages and chat room conversations).

10 FED. R. EVID. 901(b).

11 *See, e.g,. United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

12 FED. R. EVID. 901(b)(9).

contents to the sender and/or to the events. Much ESI has "built-in" authentication. Metadata, information about electronic information, is automatically attached to ESI and may serve to prove its authenticity.[13] Thus, as we write this article, our computer is storing the date of creation, the creator, the dates of the edits, the editors, the time spent editing the document and other data, which remains with the ESI in native format (for which a request now can be made pursuant to Federal Rule of Civil Procedure 34).[14] Illustrations applicable to the state analogs to Federal Rule of Evidence 901 may be found in the following decisions.

In *Hape v. State*,[15] the jury was accidentally exposed to previously undiscovered text messages in the defendant's cellular telephone when it was turned on by the jurors. The defendant's telephone was properly authenticated as having been retrieved from the defendant, so its admission into evidence was not in error.[16] The court found that the text messages stored in the telephone were "intrinsic to the cellular telephone[ ] . . . just as pages in a book belong to the book by their very nature."[17] They were also not testimonial and thus not barred as hearsay.[18] However, in the absence of precedent on the issue, the court noted that if the substance of a text message were to be offered for an evidentiary purpose distinct from that of the telephone itself, the text message, as a writing or recording, would need to be authenticated separately as per Indiana Evidence Rule 901(a).[19] While the text messages would have been presented for a separate purpose from the admission of the phone if they had been intentionally offered into evidence, their accidental presentation to the jury without proper authentication was not fundamental error, because there was compelling evidence against the defendant,

---

13 Metadata is helpful but has some frailties. See, for example, *Fennell v. First Step Designs*, 83 F.3d 526, 530 (1st Cir. 1996), which discusses saving a file to a different place and the ways that can change the metadata.

14 *See Autotech Technologies v. Automationdirect.com, Inc.*, 248 F.R.D. 556, 559 (N.D. Ill. 2008) regarding the need to make a specific request for metadata.

15 903 N.E.2d 977, 986-87 (Ind. Ct. App. 2009).

16 *Id.* at 990.

17 *Id.* at 988.

18 *Id.* at 989.

19 *Id.* at 989-90.

and it was unlikely that the content of the messages prejudiced the verdict.[20]

Another case of inadvertent failure to authenticate evidence is *Insight Technology, Inc. v. SureFire, LLC*.[21] SureFire submitted the affidavit of an undisclosed expert witness along with a compact disc of animations in support of a motion for summary judgment.[22] While it attempted to justify the inclusion of the affidavit as admissible under Federal Rule of Evidence 901 by arguing that the affidavit was used only to authenticate the animations, the court noted that Federal Rule of Evidence 901 "does not . . . make authentication evidence admissible."[23] Because SureFire failed to adhere to the expert disclosure requirements, the affidavit was stricken for purposes of summary judgment and was unavailable to authenticate the animations.[24] Citing *Lorraine v. Markel*[25] for the idea that computer animations are generally admissible "if authenticated by testimony of a witness with personal knowledge of the content of the animation," the court ruled that the animations were unauthenticated without the affidavit and thus not admissible under Federal Rule of Evidence 901, which requires authentication or self-authentication of such evidence.[26]

There are a number of cases concerning the authentication of chat logs and records of instant messages. In one such case, *United States v. Barlow*,[27] the government submitted into evidence a chat log, transcripts of online chats involving the defendant. On appeal, the defendant asserted that the government had failed to "lay a proper foundation for the . . . log prior to its admission into evidence."[28] The court held that testimony of a witness who had been involved in the chats was sufficient to authenticate the chat log, noting that other courts have come to the same conclusion, and determined that admission of the log was not plainly erroneous.[29]

---

20 *Id.* at 991.
21 No. 04-CV-74-JD, 2007 WL 3244092 (D.N.H. Nov. 1, 2007).
22 *Id.* at *1.
23 *Id.* at *1-2.
24 *Id.* at *2.
25 241 F.R.D. 534.
26 *Id.* at *3 (quoting *Lorraine*, 241 F.R.D. at 559).
27 No. 08-60556, 2009 WL 1228174, at *2-3 (5th Cir. May 6, 2009).
28 *Id.* at *2.
29 *Id.* at *3.

Courts have come to different conclusions regarding the admissibility of cut-and-paste word documents as records of chat logs, instant messages, and other electronic communications. In *United States v. Gagliardi*,[30] Gagliardi claimed that word processing files that were submitted as evidence by the government and contained cut and pasted e-mails and transcripts of instant-message chats involving him were not properly authenticated and that the trial court was in error when it admitted them. The court stated that "reasonable likelihood" is the standard for authentication and that, under Federal Rule of Evidence 901(b)(1), "[t]he testimony of a witness with knowledge that a matter is what it is claimed to be is sufficient to satisfy this standard."[31] It held that testimony of two participants in the conversations in question that the files were accurate records of the conversations was sufficient for a "reasonable juror [to] have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable," and thus were properly authenticated.[32] However, a similar document was held to be inadmissible in *United States v. Jackson*.[33]

Records of electronic conversations have presented difficulties even when they are not preserved and submitted as cut-and-paste word documents. For example, in *People v. Johnson*,[34] the court found that the admission of transcripts of online conversations in an indecent solicitation of a child case, using an undercover officer posing as a minor girl, was reversible error due to the lack of an adequate foundation for the records. To establish a proper foundation for computer-generated records as admissible business records, Illinois "requires a showing that: standard equipment was used; the particular computer generates accurate records when used appropriately; the computer was used appropriately; and the sources of the information, the method of recording utilized, and the time of preparation indicate that the record is trustworthy and should be admitted into evidence."[35]

---

30 506 F.3d 140, 151 (2d Cir. 2007).

31 *Id.*

32 *Id.*

33 488 F. Supp. 2d 866 (D. Neb. 2007), discussed *infra* in text at note 88.

34 875 N.E.2d 1256, 1260 (Ill. App. Ct. 2007).

35 *Id.* (quoting *People v. Morrow*, 256 Ill. App. 3d 392, 397 (Ill. App. Ct. 1993)).

The State did not meet this burden, because it failed to provide evidence of the investigator's competence in the use of the systems and programs used to generate the transcripts and the effectiveness of the programs themselves.[36] It also failed to lay the proper foundation for admission through witness testimony, which requires a showing of truthfulness and accuracy and that the facts were recorded closely in time to the incident.[37]

Direct printouts of electronic conversations appear to have been easier to authenticate, as in the case of *In re F.P.*[38] There, the Superior Court of Pennsylvania asserted that there is no need for new rules regarding admissibility of forms of electronic communication such as e-mail and instant messages, which "can be properly authenticated within the existing framework of Pa.R.E. 901 and Pennsylvania case law."[39] The court allowed authentication by circumstantial evidence.[40] In this case, an appeal of the conviction of a juvenile for aggravated assault, the appellant challenged a record of instant messages between a screen name belonging to the victim, who made a printout of the messages from his computer, and a person the victim believed to be the appellant.[41] The court found that the evidence "was clearly sufficient to authenticate the instant message transcripts as having originated from appellant."[42] This evidence included that, in the messages, the person using the screen name in question referred to himself by the first name of the appellant, made accusations mirroring testimony about the impetus for the assault, and referred to the fact that the victim had gone to school authorities about the online threats.[43] The appellant's contention that electronic communications are "inherently unreliable" was dismissed by the court, which pointed out that written documents involve the same kinds of uncertainties about their origins.[44]

---

36 *Id.*

37 *Id.* (quoting *Brooke Inns, Inc. v. S & R Hi-Fi & TV*, 249 Ill. App. 3d 1064, 1086 (Ill. App. Ct. 1993)).

38 878 A.2d 91 (Pa. Super. Ct. 2005).

39 *Id.* at 95-96.

40 *Id.* at 94 (citing *Commonwealth v. Brooks*, 508 A.2d 316, 318 (Pa. Super. Ct. 1986)).

41 *Id.*

42 *Id.* at 95.

43 *Id.*

44 *Id.*

Similarly, in *Adams v. Disbennett*,[45] the appellate court upheld the admission into evidence of instant messages between the parties under Ohio Evidence Rule 901(A) when the trial court permitted the plaintiff-appellee, who submitted the records, to authenticate them through his own testimony. The authenticating testimony deemed sufficient to meet the required prima facie showing included the assertion that one screen name belonged to plaintiff-appellee, the other participant was the defendant-appellant, the plaintiff-appellee had made no changes to the messages, the exhibits were computer printouts or compilations of their conversations, and the records contained information that would have been private between them.[46] The appeals court noted that the lower court was in the best position to assess the credibility of witnesses.[47] The court also found that under Ohio Evidence Rule 1001(3), which gives one definition of an "original" of computer stored data as "any printout or other output readable by sight, shown to reflect the data accurately," there was no need for the computer's hard drive to be brought into court and for the messages to be retrieved there, as contended by the defendant-appellant.[48]

Printouts of photographs from websites must also be authenticated. In a case involving unlawful sexual contact with a minor, *State v. Gaskins*,[49] an Ohio court of appeals affirmed the trial court's decision to allow the introduction of photographs of the victim posted on the website MySpace.com while prohibiting questioning about the website. The court noted that the website was not in existence prior to the incident and there was no proof that the defendant had even seen it, making questioning regarding the website irrelevant to the central question of what the defendant believed about the victim's age at the time the incident occurred.[50] However, the court permitted inclusion of the photographs themselves, because a witness testified that they were an

---

45 No. 9-08-14, 2008 WL 4615623, at *2-4 (Ohio Ct. App. Oct. 20, 2008).

46 *Id.* at *3.

47 *Id.* at *4 (citing *Seasons Coal Co. v. Cleveland*, 10 Ohio St. 3d 77, 80 (1984)).

48 *Id.*

49 No. 06CA0086-M, 2007 WL 2296454, *8 (Ohio Ct. App. Aug. 13, 2007).

50 *Id.*

accurate depiction of the victim's appearance around the time of the incident, authenticating them.[51]

Other cases with similar issues involve authentication of electronic evidence for judicial notice, as in *Schneider Saddlery Co. v. Best Shot Pet Products Int'l, LLC*,[52] a trademark infringement case. There, Best Shot submitted various unauthenticated photographs printed from the parties' web sites.[53] The court noted that, in a trademark dispute, judicial notice may be taken of "the very images that are the subject of the dispute, so long as there is no contention by either party that the images are inaccurate or could not be properly admitted before a jury"—despite the fact that courts usually hesitate to accept unauthenticated material for summary judgment purposes.[54] Therefore, images of the companies' products were admitted, because there was no dispute that they were accurate depictions of the usage of the marks.[55] However, the images from the web pages that did not fall under this exception were disregarded.[56] They did not meet the requirements that print-outs from web pages must be authenticated by presenting "evidence from a percipient witness stating that the printout accurately reflects the content of the page and the image of the page on the computer at which the printout was made."[57] The court disregarded photographs of unknown origin based on the same rationale.[58]

Automatic metadata also may create authentication problems. Each time a file is accessed, the metadata is changed to reflect the access. A person who "saves" a document in an effort to preserve it actually is altering it instead. Computer forensic experts use a system of hash marks, distinct numerical values, which identify ESI and distinguish, for example, one version of a file from another. These hash marks then serve both to authenticate and to identify the ESI. Judge Grimm admonishes:

---

51 *Id.*

52 No. 1:06-CV-02602, 2009 WL 864072, at *7 (N.D. Ohio, Mar. 31, 2009).

53 *Id.*

54 *Id.*

55 *Id.*

56 *Id.*

57 *Id.* (quoting *Nightlight Sys. v. Nitelites Franchise Sys.*, No. 1:04-CV-211, 2007 WL 4563875, at *16 (N.D. Ga. May 11, 2007)).

58 *Id.*

> A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the "final" or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. Use of hash values when creating the "final" or "legally operative" version of an electronic record can insert distinctive characteristics into it that allow its authentication under Rule 901(b)(4).[59]

You are likely to use Rule 901(b)(7) increasingly with the passage of time. That rule permits authentication by evidence that a writing authorized by law to be filed or recorded was, in fact, so filed or recorded. Computerized public records require little more than proof of public custody, which can be established through a certificate of authenticity or the testimony of the custodian or a person with knowledge that the evidence came from the custodian. For public records, reliability of the process is presumed and you need no separate proof.

In *Williams v. Long*,[60] the court provided a survey of cases and other sources discussing self-authentication of websites as official publications. It held that webpage print-outs from the Maryland Judiciary Case Search website and the Employment Standards Service website were self-authenticating under Federal Rules of Evidence 902(1) and 902(5), because the websites are both publications of a public authority, in this case the Maryland state government, and the printouts contained information, such as the websites' URLs, that served as valid identification.[61] In finding that a page printed from a restricted portion of one of the websites was self-authenticating, the court also noted that an official publication need not be "available without restriction to the general public [and that] simply because additional measures, such as [a Freedom of Information Act] request or subpoena under Fed. R. Civ. P. 45, must be employed to gain access to the publication does not mean the document is not self-authenticat-

---

59 241 F.R.D. at 547.

60 585 F. Supp. 2d 679, 686-89 (D. Md. 2008).

61 *Id.* at 689-90.

ing."[62] The court also held that the exhibits in question fell under the recognized Federal Rule of Evidence 803(8) public records exception to the hearsay rule and were thus admissible.[63]

In another case that dealt with self-authentication of printouts from a government website, *Paralyzed Veterans of America v. McPherson*,[64] the court granted the plaintiffs' request for judicial notice of documents that appeared on the website of the California Secretary of State. It noted, "It is not uncommon for courts to take judicial notice of factual information found on the world wide web," particularly for government websites.[65] The court cited the Federal Rule of Evidence 201(b) requirements for judicially noticed facts, which must not be subject to reasonable dispute as they are either generally known in the court's jurisdiction or their accuracy can be readily determined by "sources whose accuracy cannot reasonably be questioned."[66] The documents, a "letter and the Secretary of State's expressed conditions of the use of the AutoMark [voting system]," were not in dispute, nor was their accuracy reasonably questioned.[67] The court also determined that a printout of reports issued by the Office of the California Secretary of State and found on the same website were self-authenticating under Federal Rule of Evidence 902(5), because they are official records.[68]

ESI comes in a myriad of forms—e-mail, data compilations, web pages, instant messages, voicemails, digital photographs and the like. Often, a piece of evidence may be authenticated in a variety of ways. Judge Grimm advises, "there may be multiple ways to authenticate a particular computerized record, and careful attention to all the possibilities may reveal a method that significantly eases the burden of authentication."[69]

---

62 *Id.* at 690.

63 *Id.* at 690-91.

64 No. C 06-4670 SBA, 2008 WL 4183981, at *5-6 (N.D. Cal. Sept. 9, 2008).

65 *Id.* at *5 (quoting *O'Toole v. Northrop Grumman Corp.* 499 F.3d 1218, 1225 (10th Cir. 2007)).

66 *Id.*

67 *Id.* at *6.

68 *Id.* at *7.

69 *Lorraine*, 241 F.R.D. at 549.

On That You Can Rely

Hearsay is excluded, because it is deemed unreliable. Where indicia of reliability exist, the evidence may not be regarded as hearsay or an exception may apply. The sheer volume of ESI makes analysis of hearsay issues inevitable.

Hearsay is defined under Federal Rule of Evidence 801 as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." The requirement that hearsay be a *statement* by a *declarant* has significant ramifications when you analyze ESI. A statement is defined as "(1) an oral or written assertion or (2) nonverbal conduct of a person, *if it is intended by the person as an assertion*."[70] To qualify as hearsay, a statement must be an assertion intended as such. Thus, automatically generated computer information *is not hearsay* since it neither contains a statement nor does it involve a person. Images on websites or in digital photos, likewise, do not constitute hearsay unless they depict an intended message, such as a picture of a crowd of people holding signs saying "The Boss Rocks" to prove that Bruce Springsteen is a rocker. (The same digital photo would not contain hearsay if it were offered to prove that Bruce Springsteen was popular, at least in the days when this article was written.)

Even an out of court statement made by a declarant is not hearsay unless it is offered to prove the truth of its contents.[71] If it is offered for any other purpose, it ought not be excluded under this rule. Thus, an e-mail exchange that is offered to prove that the sender knew the recipient, an electronic diary entry, "I'm going to Joan's at 13 E. Point Street" offered to prove the defendant knew where the victim lived, or computerized ledger sheets showing two sets of figures for the same period offered to show tax fraud, are not hearsay. It is critical, therefore, that you painstakingly analyze the purpose for which you want to offer ESI before concluding that it is or contains hearsay.

Two other rules may exclude the evidence you seek to admit from the definition of hearsay. Although it has little unique application to ESI, when a witness is testifying at trial, Rule

---

70 FED. R. EVID. 801(a) (emphasis added).

71 FED. R. EVID. 801(c).

801(d)(1) excludes from the definition of hearsay her prior inconsistent statements taken under oath, her prior consistent statements offered to rebut a charge of recent fabrication and her identification of a person.[72] More pertinent to electronic records are admissions by party opponents, which are excluded under specified circumstances by Federal Rule of Evidence 801(d)(2). That exclusion sweeps vast quantities of e-mails from the adverse party, for example, into the admissible column. Another hearsay exclusion was utilized in *State v. Espiritu*,[73] where, at trial, the court allowed the complainant to testify about text messages, which had been lost or destroyed. The court determined that the original text messages, because they were offered to prove the truth of the matter asserted, would have been considered hearsay under Hawaii Rule of Evidence 801, analogous to Federal Rule of Evidence 801.[74] However, it also held that the text messages would have been admissible as a party admission under Hawaii Rule of Evidence 803(a)(1), qualifying as "statements offered by Respondent against Petitioner to show Petitioner's history of threats against the Complainant."[75] Extrapolating from that determination, the court stated that "[i]f evidence is hearsay, then testimony about the evidence is also hearsay," and "[c]orrespondingly, if evidence is admissible under an exception . . . then testimony about such evidence is admissible."[76]

Your conclusion that the ESI you seek to admit contains hearsay does not end your analysis. You should consider the 23 exceptions in Rule 803, which apply whether or not the declarant is available, and the five in Rule 804, which require the declarant's unavailability. Two warrant particular discussion here because of the unique issues related to ESI. The first is the state of mind exception.[77] That exception may arise frequently when you evaluate e-mails. Their informality often spurs people to "open up" in ways they would never dream of doing in more formal communications. Internet users have developed a bevy of emoticons, which pictorially display precisely the state of mind in-

---

72 FED. R. EVID. 801(d)(1).

73 176 P.3d 885, 892 (Haw. 2008).

74 *Id.* at 890.

75 *Id.* at 890-91.

76 *Id.* at 891.

77 FED. R. EVID. 803(3).

tended to accompany the words in the document. This exception may be a rich area to mine if you are seeking to offer an e-mail into evidence, and it is an exception of which to be wary if you are its opponent.

The most important exception, by far, is the business records exception recognized in Federal Rule of Evidence 803(6). That exception poses several unique problems for ESI proponents and opponents. The fundamental elements are, of course, the same: a record is admissible under this exception if (1) it was made at or near the time of the event; (2) by a person with knowledge; and (3) it was kept in the course of a regularly conducted business activity; (4) if it was the regular practice of that business activity to make the record.[78] Jack B. Weinstein and Margaret A. Berger write:

> Computerized business records are admissible into evidence under essentially the same conditions as apply to the admission of non-computerized records of a regularly conducted activity under Rule 803(6). No additional authenticating evidence is required just because the records are in computerized form rather than pen or pencil and paper.[79]

Regarding business records, in *In re Vinhnee*,[80] the court noted that, in principle, the only difference between authenticating a paperless electronic record and a paper record is "the format in which the record is maintained," placing "the focus . . . on the circumstances of the preservation of the record during the time it is in the file," assuring that the document has not been changed.

The court in *In re Vargas*,[81] referred to *Vinhnee* when discussing the admissibility of evidence under the Federal Rule of Evidence 803(6) business records exception to the hearsay rule. It noted that electronic records are covered by the same basic elements for the introduction of business records under this exception and quoted the four requirements listed in *Vinhnee* for the admission of business records under the hearsay exception:

---

78 *Id.*

79 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.08 (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 2009).

80 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005).

81 396 B.R. 511, 518 (Bankr. C.D. Cal. 2008) (quoting *Vinhnee*, 336 B.R. at 444).

> Such records must be: (1) made at or near the time by, or from information transmitted by, a person with knowledge; (2) made pursuant to a regular practice of the business activity; (3) kept in the course of regularly conducted business activity; and (4) the source, method, or circumstances of preparation must not indicate lack of trustworthiness.[82]

However, to be admitted, computer records required the provision of an eleven-step foundation by the movant, for which the court again cited *Vinhnee*:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.[83]

In this case, the movant's witness failed to meet these exacting requirements for the computer records.[84]

Cell phone records have also come to the fore as courts have deemed cell phone technology to have inherent elements of reliability. For example, in *People v. Davis*,[85] the defendant argued that using cell phone records, as admitted into evidence in the court below, to determine the location of a caller was a novelty that required a separate foundational hearing on admissibility. The court, however, noted that cell phone records had been introduced for the purpose of determining a caller's location in a number of cases "without any concern for the validity of the underlying science."[86] It also cited a then six-year-old decision that established that "'sound scientific theory' supported the use of

---

82 *Id.*

83 *Id.* (citing *Vinhnee*, 336 B.R. at 446).

84 *Id.* at 519.

85 No. A109671, 2006 WL 2965368, at *8-9 (Cal. Ct. App. Oct. 18, 2006).

86 *Id.* at *9.

[cell phone] records for that purpose . . . . [and] had been 'widely accepted.' "[87] Because "the technology in question is neither new to science or the law," the court held that a separate hearing on the admissibility of the records was not required.[88]

In another case involving cell phone records, *Wilson v. State*,[89] the Court of Appeals of Texas held that the trial court did not err when it admitted expert testimony on cellular telephones from a cellular telephone company employee under Texas Rule of Evidence 702 in a murder trial. Cellular phone records admitted as evidence "established the specific cellular towers reached by [defendant's] cellular phone on the day of the murder," and the witness testified that they "showed [defendant] traveling from the vicinity of his residence to the vicinity of the victim's residence during the time period in question."[90] The court held that even though the witness did not have "specialized expertise in cellular phone technology," her training in electronic surveillance by the company, familiarity with relevant computer programs, and work experience analyzing these kinds of records was sufficient for her both to testify as an expert under Texas Rule of Evidence 702 and to authenticate the records as their custodian under the business records exception to the hearsay rule under Texas Rule of Evidence 803(6).[91]

So much business these days is conducted through e-mail, fax and web exchanges. Care must be taken to make sure that admissibility under the business records exception is analyzed rather than simply assumed. It is not sufficient that an e-mail is generated from a business computer by an employee of a company that uses e-mails regularly. The proponent must nevertheless show that it is the regular practice of the business to make this particular type of e-mail, and the e-mail was part of the employee's regular business activity.

Embedded e-mails (strings of e-mails attached to one another) create special problems. Must each participant be conducting a regular business activity? Must each participant be required by his employer to keep this record? Must the propo-

---

87 *Id.* (quoting *Pullin v. State*, 534 S.E.2d 69, 71 (Ga. 2000)).

88 *Id.* at *10 (citing *People v. Stoll*, 49 Cal. 3d 1136, 1156 (1989)).

89 195 S.W.3d 193, 202 (Tex. Ct. App. 2006).

90 *Id.* at 196-97.

91 *Id.* at 200-02.

nent show the reliability of the computer process in addition to meeting the normal business record exception requirements?

There are no definitive answers. Some courts take a very stringent approach, *e.g., Rambus Inc. v. Infineon Tech. AG,* 348 F.Supp.2d 698, 706 (E.D.Va. 2004); others are more flexible. *United States v. Safavian*, 435 F.Supp.2d 36, 40-41 (D.D.C. 2006). A careful review of the case law in your jurisdiction is essential. If you know your trial judge, learn her proclivities in this regard. If you are not assigned to a particular judge in advance of trial, you must be prepared to meet the most demanding standards. If you are the proponent of the evidence, argue for leniency; if you are the opponent, urge exacting criteria. Above all, if you are meticulously thorough in your analysis, you will be able to meet most challenges proffered by your adversary or the court and avoid losing your argument to the intricacies and peculiarities of the old hearsay rules' application to this "new-fangled" ESI.

Never Out of Date

The final hurdle to admissibility is the set of "original writing" rules, which have required since time immemorial, that the original record be produced, if available, unless otherwise permitted.[92] Courts have tried to keep the rule up-to-date with technology and, now, a duplicate original has the same force and effect as the original.[93] Since a duplicate is any record created by means that accurately reproduce the original, rarely is there a need to obtain a true "original." Indeed, in the case of ESI, one might argue the original to be the series of 1s and 0s that the computer reads to create the image that we see, but that would hardly be useful, and there is agreement that the ESI original is "the readable display of the information on the computer screen."[94] The following cases illustrate some applications of the "original writing" rules.

In *United States v. Jackson*,[95] the court agreed with the defendant that a cut-and-paste word document of instant message conversations between the defendant and an agent of the Postal

92 FED. R. EVID. 1002.

93 FED. R. EVID. 1001(4).

94 *Lorraine*, 241 F.R.D. at 577.

95 488 F. Supp. 2d 866, 869-70 (D. Neb. 2007).

Information Service posing as a fourteen-year old girl was inadmissible as evidence. On the basis of testimony from a computer forensic expert, the court held as a matter of law that the document was not authentic because "[c]hanges, additions, and deletions have clearly been made."[96] The court also found that the document was not admissible under the best evidence rule, Federal Rule of Evidence 1002, as the expert testified about many superior methods that could have been but were not used to preserve the computer conversations.[97] The cut-and-paste document was not covered as an original under the computer printout definition, Federal Rule of Evidence 1001(3), because it did not accurately reflect the conversations, nor was it a duplicate of a true original under Federal Rules of Evidence 1001(4) and 1003.[98] In addition, even though Federal Rule of Evidence 1004 allows admission of secondary evidence when an original is destroyed, as was the case here, the court held that the document was inadmissible because "[i]t is clear that the proposed document does not accurately reflect the contents of the original."[99]

In another case involving the "original writing" rules, *State v. Espiritu*,[100] discussed above for its application of the hearsay rules,[101] the complainant testified about four text messages that were copied into a police report by hand.[102] Though the report was later typed-up, and the hand written notes lost or destroyed, the complainant used the typed report to refresh her memory.[103] The phone that contained the text messages was likewise lost or destroyed, and the complainant no longer used the same cell phone plan, making the original messages unretrievable.[104] The court held that, for the purposes of the best evidence rule, a text message is a writing, making Hawaii Rule of Evidence 1002 applicable.[105] However, the original text messages were not required in order to allow the complainant's testimony because the

96 *Id.* at 870-71.
97 *Id.* at 871.
98 *Id.*
99 *Id.*
100 176 P.3d 885.
101 *See supra* text at notes 73-76.
102 *Espiritu*, 176 P.3d at 889.
103 *Id.* at 889-90.
104 *Id.* at 892.
105 *Id.*

exception to the original writing requirement in Hawaii Rule of Evidence 1004(1) applies when originals have been lost or destroyed (not in bad faith), and the court found that bad faith could not be inferred from a "fail[ure] to preserve text messages for over two years on a cell phone for which she discontinued service," further noting that there was no indication that a printout was possible.[106] In light of the many ways that electronic evidence can be destroyed, the court also opined that Hawaii Rule of Evidence 1004(1) is well-suited to electronic evidence.[107]

Of particular interest for ESI is Rule 1004's specification of when secondary evidence may be used. The first such exception permits secondary evidence of the contents of a writing when the original is lost or destroyed. Spoliation issues aside, given the volume of ESI each of us encounters in our daily lives and the innumerable ways such evidence can "disappear," it is not surprising that courts have recognized the application of this exception.[108]

Finally, the rule with, perhaps, the greatest applicability to ESI is Rule 1006, which permits the introduction of summaries in lieu of voluminous writings so long as the original writings were made available to the adverse party.[109] Imagine having to haul to court your client's entire database every time you wanted to establish its results. But there is no such requirement. You need only prepare, or have prepared, a chart, summary or calculation with the information you need. It is that summary that becomes the evidence in the case, although the court is given the authority in the rule to require the presence of the original writing.[110]

No Matter What the Future Brings

Now that you have explored these rules and how they adapt to ESI, how can you use them to your advantage in your future cases? A hypothetical can best demonstrate their practical application.

In this hypothetical, the plaintiff has presented its case, the gist of which is that, on the weekend before competing presenta-

106 *Id.*
107 *Id.* at 892-93 (citing *Lorraine*, 241 F.R.D. at 580).
108 *Lorraine*, 241 F.R.D. at 580.
109 FED. R. EVID. 1006.
110 *Id.*

tions to a potentially huge buyer, WidgetsWise posted disparaging remarks on its website about Company Plaintiff and its products. The CEO of the target company was doing his "homework" over the weekend and saw the disparaging information. Although he permitted Company Plaintiff to make its presentation, he had, more or less, decided he did not want to do business with that company and awarded the contract to WidgetsWise. Mr. Pro is the proponent of the webpage he wants to offer into evidence to prove that his client did not disparage the plaintiff on the web. Ms. Opp seeks to exclude the evidence or, at least, diminish its value. The witness, Mr. Geek, is the company's webmaster.

Mr. Pro: I show you Exhibit 1 for identification, can you tell me what it is?

Mr. Geek: It is a printout of my company's webpage for June 4, 2005, the date we were supposed to have posted something derogatory about Company Plaintiff.

Mr. Pro: How do you know that that's what the page is, sir?

Mr. Geek: I am the webmaster, and it is my job to create and maintain the content of my company's website, www.widgetswise.com. I retrieved it and printed it from a backup tape that archives our web pages every five days.

Mr. Pro: How does WidgetsWise use its website?

Mr. Geek: It's a regular part of WidgetsWise's marketing efforts. Our customers come to the web, and they can see our inventory. They can even order online. As a result, it's very important that we keep our website up-to-date and accurate.

Mr. Pro: How often do you work on the site?

Mr. Geek: I'm always doing something on the site seven hours a day, five days a week.

Mr. Pro: Does anyone else post content to the site?

Mr. Geek: No, it is password protected, and I am the only web programmer in the company.

Mr. Pro: Does anyone else remove content from the site?

Mr. Geek: Same answer. I am the one who originally created the site, and, to my knowledge, I am the only one who makes changes to it. If someone at the company wants something posted or deleted, they give it to me.

Mr. Pro: Can anyone from the outside tamper with the content?

Mr. Geek: No, sir. We have three levels of security that I personally designed [which he describes].

Mr. Pro: Is Exhibit 1 an accurate representation of the website as it appeared at the relevant time?

Mr. Geek. Yes, it is.

When the document is offered into evidence, Ms. Opp asks for and is given the opportunity to voir dire the witness.

Ms. Opp: When you're doing your work, you go to the pages you need to modify, isn't that right?
Mr. Geek: Yes.
Ms. Opp: In fact, there are days when you work exclusively on a single page, aren't there?
Mr. Geek: Yes.
Ms. Opp: And, on those days, you don't view the other pages at all, do you?
Mr. Geek: No.
Ms. Opp: You testified that your backup tape from which you printed Exhibit 1 archives the pages every five days, isn't that right?
Mr. Geek: Yes.
Ms. Opp: You can't tell me if it archived this page on June 4, 2005, can you?
Mr. Geek: No, but I can say it's within five days of that date.
Ms. Opp: So the system could have archived the page on June 3, 2005, and then it wouldn't archive it again until June 8, isn't that correct?
Mr. Geek: Yes.
Ms. Opp: You don't access your company's website in your spare time, do you?
Mr. Geek: Heck, no. I have enough of it during the week.
Ms. Opp: So if someone were to access the site on the weekend, post something, leave it there for 48 hours and then remove it, you wouldn't have seen it would you?
Mr. Geek: No, but it would leave a trail.
Ms. Opp: But since you believe you're the only one who accesses the content of your website, you don't regularly look at that information, do you?
Mr. Geek: No.
Ms. Opp: You didn't look to see if there was a trail left by another user on June 4, 2005, did you?
Mr. Geek: No.
Ms. Opp: So, as you sit here today, you can't tell me for sure whether another user accessed the content of that site on June 4, 2005, can you?
Mr. Geek: No, ma'am, except for the fact that no one ever does.
Ms. Opp: To your knowledge.
Mr. Geek: Yes, to my knowledge.
Ms. Opp: And, in fact, you're not the only one that has the password, are you?

Mr. Geek: No, of course not. The CEO of our company has it, the head of human resources has it, and the security officer has it.
Ms. Opp: The CEO is relatively new, isn't she?
Mr. Geek: Yes.
Ms. Opp: She's the one that used to work for Company Plaintiff, isn't she?
Mr. Geek: Yes.
Ms. Opp: She's the same one that was fired from Company Plaintiff, isn't she?
Mr. Geek: Yes.
Ms. Opp: Now with her password, she could access the content of the website, couldn't she?
Mr. Geek: Yes.
Ms. Opp: And she could add content, if she wanted to, and remove it too, couldn't she?
Mr. Geek: Yes, but as I stated, nobody accesses the content of the website but me.
Ms. Opp: To your knowledge.
Mr. Geek: Yes, to my knowledge.
Ms. Opp: Sir, you can't say specifically that you saw this content in Exhibit 1 on your company's website on Saturday, June 4, 2005, can you?
Mr. Geek: Well, I guess not, but . . . .
Ms. Opp: And you can't exclude the possibility that someone else from your company posted disparaging remarks on your website that day, can you?
Mr. Geek: Well, I guess not, but I'm . . . .
Ms. Opp: No further questions.

Even this simplistic hypothetical is useful to demonstrate the application of the rules to ESI. The proponent lays an adequate foundation for admission of the webpage. The webpage is at the very heart of the matter, so it is both relevant and not unduly prejudicial under Federal Rules of Evidence 401 - 403. Mr. Pro uses a person with knowledge to authenticate the webpage under Rule 901(b)(1) and to demonstrate its reliability. He *is* offering to prove the contents of a writing, so he is required to use an "original" pursuant to Federal Rule of Evidence 1002. Since printouts of ESI constitute originals, he satisfies that requirement.[111] The proponent shows that the website is maintained in the ordinary course of WidgetsWise's business and that it is part of WidgetsWise's regular practice to make such records, thus sat-

111 FED. R. EVID. 1002.

isfying the business records exception to the rule against hearsay.[112] Following direct, the webpage is likely admitted in most, if not all, courts.

The cross, however, makes the webpage's admission doubtful. Ms. Opp attacks only one element of the foundation for admissibility—authentication. But she is able to undercut every aspect that Mr. Pro needs. While Mr. Geek unquestionably is a person with knowledge of the website, he admits he has no knowledge of the particular webpage for the particular day. It is even questionable whether the printout *is* for the right day, as the backup is generated only every five days, and there is no testimony as to whether it captured June 4, 2005. Most importantly, Ms. Opp is able to challenge Mr. Pro's showing of reliability. She establishes that others had access to the website, that Mr. Geek would be unaware of such access and that, in addition to the simple profit motive, WidgetsWise's CEO might well have had revenge on her mind on the date in question. *Is* the webpage what Mr. Pro purports it to be? We'll let you be the judge.

A Case of Do or Die

Admissibility of ESI underscores the adage that everything old is new again. We must apply the familiar rules to types of evidence not even contemplated when the rules were written. Yet, those rules are sufficiently adaptable to those who are prepared. And prepare we must. Judge Grimm cautions:

> The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues [relevance, authenticity, hearsay, original writing and unfair prejudice] that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, *counsel should know how to get it right on the first try*.[113]

---

112 FED. R. EVID. 803(6).

113 *Lorraine*, 241 F.R.D. at 585 (emphasis added).

You Must Remember This

There is a well known exchange in the movie, *Casablanca*, between Rick (Humphrey Bogart) and Renault (Claude Rains):

RENAULT: What in heaven's name brought you to Casablanca?
RICK: My health. I came to Casablanca for the waters.
RENAULT: Waters? What waters? We're in the desert.
RICK: I was misinformed.[114]

When it comes to the admissibility of ESI, don't be misinformed.

114 Julius J. Epstein, Philip G. Epstein, Howard Koch, *Casablanca* (1942).