

Getting It In: The Admissibility of Electronically Stored Information in Employment Litigation

Jocelyn D. Larkin
Director of Litigation and Training
Impact Fund
125 University Avenue, Suite 102
Berkeley, CA 94710
(510) 845-3473, ext. 306
jlarkin@impactfund.org

“Be careful what you ask for . . . because you might actually get it.”
Lorraine v. Markel American Insurance Co., 241 F.R.D. 534, 537 (D. Md. 2007)

With much fanfare, the Federal Rules of Civil Procedure were amended in December 2006 to accommodate the discovery of electronically stored information (ESI). The rule amendments reflected the reality that the evidence in virtually every piece of civil litigation now involves information stored in electronic form. In employment litigation today, e-mail messages, personnel databases and website content often form the evidentiary core of an employee’s case. In response to the new discovery rules, practitioners dutifully signed up for continuing legal education programs to learn the minutiae of e-discovery. What was largely neglected, however, was an equally important question: once you’ve gone to the trouble and expense of obtaining electronic information, how do you get it into evidence at trial or in response to a summary judgment motion?

An enormously helpful guide to this multi-faceted question comes from a very unlikely source – a dispute arising from a lighting storm that damaged a private yacht anchored in the Chesapeake Bay. In *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 537 (D. Md. 2007), the parties filed competing summary judgment motions

to enforce a private arbitration award but both sides failed to authenticate *any* of the documentary evidence submitted, including copies of critically important e-mail messages. The magistrate judge used this somewhat improbable scenario to author a comprehensive and valuable primer on the admissibility of ESI. This article uses the *Lorraine* decision to explain the essential framework for analyzing ESI admissibility questions and to highlight some practical tips for addressing these issues in the employment law context.

I. ESI and Employment Litigation

When employment lawyers think about electronic evidence, they understandably focus on e-mail. Without a doubt, the casual and spontaneous exchange of e-mail in the workplace has proven tremendously useful for demonstrating discriminatory motive or intent. Predictably, though, electronic communication methods are rapidly evolving and litigators must also be thinking about the admissibility of instant messages, text messages, blog posts, project “wikis,” calendar programs, and social networking sites.

There are, moreover, many other forms of electronic information that may be relevant in employment litigation. For example, a discriminatory hiring case could involve a job announcement drafted by an employer, which is then posted on an internet website hosted by a third-party (like Monster.com), and resumes submitted by the plaintiff and his comparators in response. A wage and hour claim for a package delivery driver could implicate dispatch reports, payroll records, employee badge swipes on the company’s timekeeping system, public toll road and bridge “fast pass” records, and customer signatures on handheld devices (to demonstrate when packages were received).

While all of these bits of ESI should be admissible, practitioners must anticipate and plan their strategy for clearing the key evidentiary hurdles.

II. ESI Admissibility Hurdles

There are “five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence. . . .” *Lorraine*, 241 F.R.D. at 585.

Those issues are:

- ✓ Relevance (Fed. R. Evid. 401);
- ✓ Authenticity (Fed. R. Evid. 901 and 902)
- ✓ Hearsay (Fed. R. Evid. 801, 803, 804, 807)
- ✓ Original Writing, a.k.a. Best Evidence Rule (Fed. R. Evid. 1001 – 1008)
- ✓ Unfair Prejudice (Fed. R. Evid. 403)

A. Relevance

Let’s start with an easy one – proving that a piece of electronic evidence is relevant. Evidence is relevant if it tends to make the existence of any fact more or less probable than it would be without the evidence. Fed. R. Evid. 401. ESI typically raises no unique problems of relevance. So, for example, a snapshot of available job openings on a company’s website would be relevant to show that the reason that an employer gave for terminating an employee (i.e. downsizing) was pretextual. A snapshot of the home page of the website would be relevant background evidence to put the job openings page in context for the jury. Remember that evidence may be relevant for more than one purpose and that advocates should articulate multiple theories. Or, as Magistrate Grimm put it in *Lorraine*, don’t put all your “eggs in a single evidentiary basket.” *Id.* at 541.

B. Authenticity

A party must also demonstrate that a piece of electronic evidence is authentic. The authentication requirement “is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.” Fed. R. Evid. 901(a). The proponent need not *prove* authenticity, only make a *prima facie* showing. *Lorraine*, 241 F.R.D. at 542.

The Manual for Complex Litigation highlights some of the unique concerns about the accuracy and authenticity of ESI:

Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling.

Manual for Complex Litigation §11.446 (4th ed. 2000). Those concerns may be heightened when data has been processed, rather than just stored. As a result, the extent of the showing necessary to authenticate a piece of electronic evidence will depend on the nature of the evidence and its evidentiary purpose.

Federal Rule of Evidence 901(b) provides a non-exclusive list of examples of means to authenticate evidence. Several of these illustrative methods will be of particular importance for electronic evidence.

1. *Testimony of a Witness*

A common approach to authentication will be through the direct evidence of a witness with knowledge. Rule 901(b)(1) suggests authentication by means of “[t]estimony that a matter is what it is claimed to be.” Very simply, a witness could testify that she recognizes a copy of an e-mail that she drafted or received. An authenticating witness need not have personal knowledge of the particular exhibit if he

can attest to “the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change. . . .” *Lorraine*, 241 F.R.D. at 545. For example, a webmaster could authenticate snapshots of web pages from a corporate website that he maintains, even if he did not create the content.

2. *Comparison by Trier or Expert Witness*

Federal Rule of Evidence 901(b)(3) permits authentication by means of “[c]omparison by the trier of fact or expert witness with specimens which have been authenticated.” So, if one e-mail from a decision-maker has been properly authenticated, a second e-mail could be authenticated through comparison with the first. *See U.S. v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

3. *Distinctive Characteristics*

Federal Rule of Evidence 901(b)(4) is “one of the most frequently used to authenticate e-mail and other electronic records.” *Lorraine*, 241 F.R.D. 546. It allows for authentication by “[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances” – in other words, through circumstantial evidence. *Id.* For example, the presence of a party’s name and e-mail address may help establish the authenticity of an e-mail. Getting a little more technical, electronic documents, in their native format, contain a wide range of “metadata,” such as a file’s name, location, format, size, creator, time and date created, and modification history. *Id.* Metadata is, thus, a distinctive characteristic, useful for the authentication of ESI.

The *Lorraine* court acknowledged an important point about which the reader may already be puzzling – isn’t electronic information easily susceptible to hacking or

tampering, undermining the authentication process? Or, more simply, unless someone witnessed an individual actually writing an e-mail, how do we know that a computer terminal wasn't accessed by an unauthorized person to download forbidden material or send a disputed e-mail? While metadata is not "foolproof," it can be used to make a *prima facie* showing necessary for authentication and threshold admissibility. *Id.* The ultimate determination of the information's authenticity will be a question of fact, determined by the jury, just as it would be for a paper document claimed to be forged.

4. *Public Records or Reports*

Public records may be authenticated by proof of custody, without also showing reliability or accuracy. *Lorraine*, 241 F.R.D. at 548. Rule 901(b)(7) offers this example, which expressly anticipates electronic records:

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

Emphasis added. Fed. R. Evid. 901(b)(7). Custody may be established by a certificate of authenticity from the public office or through the testimony of the custodian or other witness with knowledge that the evidence is from a public office authorized by law to keep such records. *Lorraine*, 241 F.R.D. at 548. As discussed below, some public records may also be self-authenticated.

5. *Process or System*

Federal Rule of Evidence 901(b)(9) permits "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result" for authentication. Ideally suited to computer-generated evidence, this

approach uses a witness to explain the operation of the computer system or process as well the protocols for maintenance and testing to ensure reliability.

6. Self-Authenticating Documents

Federal Rule of Evidence 902 provides twelve categories of documents that require no extrinsic evidence to establish their authenticity. The three most relevant for ESI purposes are official publications, trade inscriptions, and certified domestic records of regularly conducted business.

“[P]ublications purporting to be issued by public authority” are self-authenticating. Fed. R. Evid. 902(5). This provision is very useful for employment litigation because it permits the admission of government labor or other population statistics. In *E.E.O.C v. E.I. DuPont de Nemours and Co.*, 2004 WL 2347556 (E.D.La. Oct. 18, 2004), print-outs of information from the U.S. Census Bureau website were admitted into evidence under this method.

Information that bears a company logo may also be self-authenticated under Rule 902(7) for “[i]nscriptions, signs, tags or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.” For example, a company identifier on an e-mail or website screenshot may be sufficient to authenticate it. *Lorraine*, 241 F.R.D. at 551-52.

Finally, Rule 902(11) permits authentication of business records without a foundation witness, if the exhibit is accompanied by a declaration of its custodian. Notice to adverse parties is required. Fed. R. Evid. 902(11).

7. Admissions, Stipulations and Pretrial Disclosures

The Federal Rules of Civil Procedure provide at least three ways to authenticate electronic evidence before trial. A party may use requests for admission to authenticate ESI in the discovery process. Fed. R. Civ. P. 36 (a)(1)(B). At a pre-trial conference, a party may propose stipulations about the authenticity of ESI about which the court may take “appropriate action.” Fed. R. Civ. P. 16(c)(2)(C). Finally, once a party makes its pre-trial disclosures under Fed. R. Civ. P. 26(a)(3) identifying each exhibit, the opposing party has fourteen days to serve and file objections to the admissibility of any exhibit. Most evidentiary objections not timely made are waived. *Id.* These methods provide a terrific opportunity to foreclose authenticity objections, but require advanced planning.

8. More Creative Approaches to Authentication

A party may seek judicial notice of foundational facts needs to authenticate an electronic document. Fed. R. Evid. 201(b).

Judicial notice could be a helpful way to establish certain well known characteristics of computers, how the internet works, scientific principles underlying calculations performed within computer programs, and many similar facts that could facilitate authenticating electronic evidence.

Lorraine, 241 F.R.D. at 553.

Courts have suggested that records produced in discovery by the opposing party are presumptively authentic, thereby shifting the burden of authentication to the producing party challenging their reliability. *Indianapolis Minority Contractors Ass’n, Inc., v. Wiley*, 1998 WL 1988826, *6 (S.D. Ind. May 13, 1998).

Acknowledging that the evidence did not squarely fit within any of the existing authentication examples, one court allowed an expert witness from an internet archive service (sometimes called “the wayback machine”) to authenticate documents that purported to be versions of the defendant’s website as it appeared on various dates in

question. *Telewizja Polska USA, Inc. v. EchoStar Satellite Corp.*, 2004 WL 2367740 *5 (N.D. Ill. Oct. 15, 2004).

C. Hearsay

To analyze hearsay questions, practitioners must address five issues:

- ✓ Is there a *statement*? (Fed. R. Evid. 801(a))
- ✓ Was the statement made by a *declarant*? (Fed. R. Evid. 801(b))
- ✓ Is the statement *offered for the truth* of its contents? (Fed. R. Evid. 801(c))
- ✓ Is the statement *excluded* from the definition of hearsay? (Fed. R. Evid. 801(d))
- ✓ Is the statement covered by a hearsay *exception*? (Fed. R. Evid. 803, 804 or 807)

Electronic evidence often does not qualify as hearsay. Cases have held that electronic reports generated by a computer, such as a fax machine report, are not hearsay because there is neither a statement nor a declarant. *Lorraine*, 241 F.R.D. at 564-65. Often ESI is offered for a purpose other than to prove the truth of its contents, such as to show motive or state of mind. *Id.* As with regular documents, much electronic information will be excluded from the definition of hearsay as the admission of a party-opponent. Fed. R. Evid. 801(d)(2).

Of the over two dozen hearsay exceptions, several have particular relevance to electronic evidence. Exceptions for “present sense impression” and “excited utterance” may be useful for instant or text messages. See Fed. R. Evid. 803(1) & 803(2). As the *Lorraine* court noted:

The prevalence of electronic communication devices, and the fact that many are portable and small, means that people always seem to have their laptops, PDA’s,

and cell phones with them, and available for use to send e-mails or text messages describing events as they are happening.

Id. at 569. Similarly, the exception for “existing state of mind” may be particularly useful for e-mail, “a medium of communication that seems particularly prone to candid, perhaps too candid, statements of the declarant’s state of mind, feelings, emotions, and motives.” *Lorraine*, 241 F.R.D. at 570; Fed. R. Evid. 803(3). An e-mail or text message that demonstrates discriminatory intent or animus towards the plaintiff, which does not otherwise qualify as a party admission, might be admissible in this way.

The hearsay exception for business records is often invoked for electronic records. Fed. R. Evid. 803(6). It can be particularly useful to secure admission of e-mail chains, which may involve multiple layers of hearsay. *Lorraine*, 241 F.R.D. at 572. To qualify for this exception, the e-mail must be in furtherance of the business’ needs, and not for personal use. This distinction is not always obvious: if the sales manager forwards to the sales team an e-mail which includes a racist joke to ‘keep morale up,’ is that in furtherance of business needs or personal? The case law on the application of the business records exception to ESI varies significantly – from lenient to very demanding -- so practitioners should do the research in their jurisdiction before relying on this exception. *Id.*

Finally, government websites and other electronic records may be admitted under the public records hearsay exception. Fed. R. Evid. 803(8). See *E.E.O.C v. E.I. DuPont de Nemours, supra*.

D. Original Writing

The Original Writing Rule (Fed. R. Evid. 1001 – 1008), traditionally known as the Best Evidence Rule, applies only when an original or duplicate is being used to prove

the contents of a writing. Fed. R. Evid. 1002. The rules have largely eviscerated any distinction between originals and duplicates, and particularly for electronic records. “If data are stored in a computer or similar device, any printout or output readable by sight, shown to reflect the data accurately, is an ‘original’.” Fed. R. Evid. 1001(3). Secondary sources can, moreover, be used to prove the content of writings if the originals have been lost or destroyed. Fed. R. Evid. 1004. Practitioners may need to avail themselves of this alternative “[g]iven the myriad ways that electronic records may be deleted, lost as a result of system malfunctions, purged as a result of routine electronic records management software. . . .” *Lorraine*, 241 F.R.D. at 580. If an employer has deleted necessary records, and a court is unwilling to order issue preclusion, an employee plaintiff may need to retain a forensics expert to reconstruct the content of records where possible.

ESI may also be admitted under Rule 1006, which permits the presentation of a summary or chart of voluminous records. This practical tool may be used only if the originals or duplicates are made available for examination by the other parties. Fed. R. Evid. 1006. Employment litigators will make frequent use of this provision to summarize payroll, personnel or time records.

E. Unfair Prejudice

The final evidentiary hurdle is Federal Rule of Evidence 403, which requires a trial judge to balance the probative value of the evidence against the potential for unfair prejudice or harm. One form of electronic evidence, computer animations, implicates the policy concerns underlying Rule 403, because a jury may mistake the simulation for the

actual events. Computer animations are not typically used in employment litigation, however.

III. Conclusion

Despite the ubiquity of ESI, there is relatively little published case precedent regarding its admissibility, and even less focused on the issue in the employment law context. Moreover, some of the early ESI admissibility cases reflect undue suspicion about the reliability of electronic evidence. One would expect that, as trial judges become more accustomed to the introduction of electronic information into evidence, some of this mistrust will diminish. In the meantime, practitioners should carefully plan their strategy for ensuring that they can admit this valuable and varied source of evidence.

Checklist for Admissibility of Electronically Stored Information (ESI)

