New York Law Journal
TODAY
TECHNOLOGY
Tuesday, October 23, 2007
ALM

Overcoming Evidentiary Hurdles

• ELECTRONIC DISCOVERY •

Litigation counsel should consider at an early stage not only how to obtain electonically stored information, but also how to secure—or challenge—its admission into evidence. In the electronic sphere, as elsewhere, the fruits of discovery do not inevitably constitute competent evidence.

BY H. CHRISTOPHER BOEHNING AND DANIEL J. TOAL

Recent revisions to the Federal Rules of Civil Procedure have focused on the discovery and production of electronically stored information. As alluring as the promise of discovering a smoking-gun e-mail is, such an e-mail only becomes useful in litigation if it can surmount a series of evidentiary hurdles that all too often receive only scant attention and, in many cases, are overlooked entirely.

The latter was the case in *Lorraine v. Markel American Ins. Co.*[1] On the night of May 17, 2004, lightning struck Jack Lorraine's yacht, Chessie, as it sat at anchor in Chesapeake Bay. Chessie's hull sustained serious damage, which ultimately led to Lorraine and his insurance company, Markel, contesting the scope of an arbitration agreement into which both had earlier entered.

H. Christopher Boehning *Daniel J. Toal*

Appearing before Chief Magistrate Judge Paul W. Grimm in the U.S. District Court for the District of Maryland, both Lorraine and Markel moved for summary judgment, each relying heavily on e-mail exchanges appended to their respective motions. Neither party, however, made any effort to authenticate the e-mails. Nor did they consider, let alone address, any of the hearsay issues raised by these e-mails. The parties also ignored the potential implications of the original writings rule.

This utter disregard for these evidentiary issues led the magistrate judge to dismiss both motions. It also prompted him to issue a 50-page opinion that reads as part cautionary tale and part primer on evidentiary issues related to e-discovery. In addition to providing a general reminder that the rules of evidence apply to electronically stored information (ESI), the decision highlights some areas of the rules of evidence that are particularly important for litigators to keep in mind when dealing with ESI.

The rules of evidence relating to authenticity are among the principal obstacles to admission of an electronic document into evidence. Paper documents, some courts have reasoned, can be examined for signs of physical alteration or forgery. Electronic documents, by contrast, are more easily modified without readily apparent signs of alteration. And while some courts therefore have scrutinized electronic documents more carefully, the requirements under the Federal Rules of Evidence for authentication of electronic and "hard copy" documents are one and the same.

The general authentication provision, Rule 901(a), requires only that the party moving to introduce the document into evidence show "evidence sufficient to support a finding that the matter in question is what its proponent claims." Though this is not a particularly exacting standard, Magistrate Judge Grimm noted that "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."[2] Such a potentially fatal mistake can be avoided with a bit of care and forethought.

H. Christopher Boehning and **Daniel J. Toal** are litigation partners at Paul Weiss, Rifkind, Wharton & Garrison LLP. **Joshua D. Kaye,** a litigation associate at the firm, assisted in the preparation of the article.

Rule 901(b) sets out a non-exclusive, illustrative list of methods by which evidence can be authenticated. While some methods, like 901(b)(2), which allows for authentication by nonexpert opinion on handwriting, are unlikely to be useful when dealing with ESI, other authentication techniques are particularly well suited to ESI and should be given careful consideration when preparing to authenticate (or oppose the authentication of) an electronic document.

• **Authentication through testimony**

Rule 901(b)(1) allows authentication through testimony by a witness with knowledge "that a matter is what it is claimed to be." At its most straightforward, such a witness could be the author of the exhibit. In the alternative, the authenticating witness could be a non-drafter with "personal knowledge of how that type of exhibit is routinely made," which generally requires the witness to be able to testify with specificity about the process by which the ESI is created, acquired, maintained, and preserved without alteration or change. On the other hand, "boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule...or public record exception" will not suffice.[3]

• **Circumstantial authentication**

Rule 901(b)(4) is the most common method for authenticating e-mail and other electronic records. This rule allows for authentication by "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Under this rule, an e-mail can be authenticated by, for example, considering the e-mail address of the purported sender and the fact that the apparent author would have been familiar with the content of the e-mail.

• **Preparing for circumstantial authentication**

Clients concerned about ensuring that they will be able to introduce their own ESI in future litigation can plan ahead to make use of Rule 901(b)(4) by adopting a system of assigning "hash values" to finished documents.

A "hash value," or "hash mark," is a series of numbers created by applying characteristics from a specific file to a standard mathematical algorithm. The resulting number is unique and can serve as that file's "digital fingerprint." In addition to allowing for relatively straightforward authentication of legitimate documents, hash values also can help guard against opponents attempting to introduce earlier versions of a document as final.[4]

• **Authentication by comparison**

Another frequently used method of authenticating ESI is set out in Rule 901(b)(3), which allows for authentication by comparison of the proposed evidence with an already authenticated document, either by an expert witness or the trier of fact. Several courts have held that e-mails that cannot be authenticated otherwise may be authenticated by having the fact finder compare the e-mails with specimens authenticated by other methods, such as those discussed above and below.[5]

• **Self-authentication**

Some documents are self-authenticating under Rule 902. One category of documents for which self-authentication is permitted in particular should be given special consideration when dealing with ESI. Rule 902(7) allows self-authentication for documents that bear "inscriptions, sign, tags or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin." Though this has not been frequently litigated,[6] this rule may permit authentication of business e-mails with "information showing the origin of the transmission and identifying the employer-company."[7] Thus, an automatic signature at the end of an e-mail may be enough for self-authentication.

Hearsay

After ESI evidence has passed the authentication hurdle, counsel must then consider whether there are any hearsay issues.

The first issue to consider is whether the electronic information sought to be introduced is hearsay at all. Hearsay is an out-of-court statement made by a declarant and offered for the truth of the matter asserted.

Under Rule 801(a), a "statement" is "(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion." A "declarant" is "a person who makes a statement." Notice that both of these definitions specifically refer to a "person."

This has the effect of excluding anything automatically generated by a computer. So, for example, a time stamp automatically added to an e-mail showing the date and time at which it was sent would be outside the definition of hearsay. Though there could still be evidentiary issues related to the e-mail, the hearsay rule should not bar the time stamp from being introduced into evidence for the truth of the matter asserted (i.e., that it was sent when the timestamp says it was).

If an electronic document is hearsay, consideration should be given to whether any exceptions to the hearsay rule might apply. Courts continue to define how the contours of the hearsay exceptions apply to ESI. Many of the exceptions, as well as the exclusions from the definition of hearsay, are applied to ESI in a wholly conventional matter.

The admission of the party-opponent exclusion under Rule 802(d)(2)(A), for example, is applied to e-mails made by a party in the same way that it would be to a verbal statement or a handwritten note.[8] There are other hearsay exceptions, however, to which careful thought should be devoted in the context of ESI.

Business Records Exception

The "business records" exception to the hearsay rule allows the admission of a document that was made in the normal course of business, at or near the time of the events it records, and that was based on either the personal knowledge of the author or a person who had a business duty to transmit that information to the author.

Given the overwhelming predominance not only of e-mail, but also electronic record-keeping in many industries, it is not surprising that this is one of the most frequently argued hearsay exceptions when the admissibility of electronic evidence is at issue.

Courts, however, have not been uniform in their application of the business records exception. Some jurisdictions, for example, have required each e-mail in an e-mail chain to independently satisfy the business records exception, or some other exception, in order

to be admissible. Other courts have been more lenient, admitting e-mail chains as a whole and leaving for the jury the ultimate question of trustworthiness.[9]

Novel Hearsay Exceptions

Because e-mails tend to be much more informal than other writings and—with the proliferation of BlackBerries and other hand-held e-mail devices—are written from just about every place imaginable, courts have begun to consider the use of hearsay exceptions that have not typically been used for other writings.

• Present sense impression

Rule 803(1) allows admission of a statement that would otherwise be excluded by the hearsay exclusion if it is a "present sense impression." The rule defines a present sense impression as "a statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter." Though courts have not yet had much opportunity to consider this question,[10] it is not difficult to imagine scenarios in which this rule could be successfully used as the basis for admission of an e-mail or text message describing an ongoing event.

• Excited utterance

Closely related to the present sense impression exception is the excited utterance exception. Rule 803(2) sets out a hearsay exception for "a statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition." Thus far no court that has considered this rule in the context of an e-mail or text message has found it applicable. Nor have those courts held, however, that e-mails, as a category, are incapable of satisfying the excited utterance exception. The courts that have considered the question instead have merely determined that, in the particular circumstances of those cases, the e-mails in question did not qualify as excited utterances.[11]

• Then-existing mental, emotional or physical condition

Rule 803(3) provides a hearsay exception for "a statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health)." Like the present sense impression and excited utterance exceptions, the requirement of a contemporaneous statement makes this exception particularly well-suited to the quickly written, off-the-cuff nature of many e-mails.[12]

Original Writings Rule

The "original writings" rules require that an original writing, recording or photograph be provided in order to prove its contents.[13]

A duplicate is also admissible, however, unless a genuine question is raised as to the authenticity of the original or it would be unfair to admit the duplicate. Because courts have typically found that the "original" of information stored in a computer is any readable form of that information, so long as it accurately reflects the data, this rule is not commonly litigated in the context of electronically stored information.

Still, it is an issue worthy of consideration, particularly when appearing before judges who may be less comfortable with the idea of evidence being drawn straight from seemingly nebulous digital storage media and placed directly into evidence.

Conclusion

All of these evidentiary issues are, of course, important in the context of trial. As the *Lorraine* decision underscores, however, they are equally important when preparing motions for summary judgment.

Clearing the evidentiary hurdles using any of these methods could mean the difference between a successful motion and the uncertainty of a trial. In order for a court to consider evidence in a motion for summary judgment, the evidence must be submitted in a form that would be admissible at trial. Thus courts typically will not consider unsworn, unauthenticated documents on a motion for summary judgment; documents must be authenticated by and attached to an affidavit that meets the requirements of Rule 56(e).

In view of the increasing focus on electronic discovery, litigation counsel are well advised to consider at an early stage not only how to obtain electronically stored information, but also how to secure—or challenge—its admission into evidence. In the electronic sphere, as elsewhere, the fruits of discovery do not inevitably constitute competent evidence.

•••••••••••••●●●•••••••••••••

1. *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).
2. Id. at 542.
3. Id. at 545.
4. Id. at 546-7; see also *Williams v. Sprint/United Mgmt. Co.*, 203 F.R.D. 640, 655 (D. Kan. 2005).
5. See, e.g., *United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).
6. *Superhighway Consulting, Inc. v. Techwave, Inc.*, 1999 WL 1044870 (N.D. Ill. Nov. 16, 1999).
7. *Lorraine*, 241 F.R.D. at 551.
8. See *Safavian*, 435 F.3d at 43-44.
9. Compare *State of New York v. Microsoft*, 2002 WL 649951 (D.D.C. April 12, 2002); *Rambus Inc. v. Infineon Tech. AG*, 348 F.Supp.2d 698 (E.D.Va. 2004) with *Safavian*, 435 F.Supp. 2d. 36 (D.D.C. 2006).
10. See *United States v. Ferber*, 966 F.Supp. 90 (D. Mass. 1997) (admitting an e-mail written by a co-worker "soon, very soon" after a phone conversation with the defendant recounting their conversation under the present sense impression exception to the hearsay rule); *Westfed Holdings, Inc. v. United States*, 55 Fed. Cl. 544, 566-7 (2003) (court considers argument that e-mails were admissible under the present sense impression hearsay exception but does not allow admission because the defendant could not show that the e-mails were contemporaneous or near-contemporaneous.), rev'd in part on other grounds, 407 F.3d 1352 (Fed. Cir. May 12, 2005).
11. *Ferber*, 966 F. Supp. at 99 (finding that e-mail did not qualify as an excited utterance even though it ended with "My mind is mush!" and author was "very upset, panicked" when he wrote it because the "detail, the length, the possibility [the author] spoke to this Kevin before he wrote it, all of it signals to me that whatever he may say about his mind being mush, there's ample time for him to reflect, fabricate.").
12. See, e.g., *United States v. Safavian*, 435 F.Supp. 2d at 44 (D.D.C. 2006); *Leelanu Wine Cellars, Ltd. v. Black & Red, Inc.*, 452 F.Supp. 2d 772, 786 (W.D. Mich. 2006); *State of New York v. Microsoft*, 2002 WL 649951 (D.D.C. April 12, 2002).
13. F.R.E. §§1001-03.