

ESI: You Have It, But Can You Use It?

By Seth D. Rothman and Lisa J. Hart, Hughes Hubbard & Reed LLP

With all the news last year about spoliation and sanctions, it is sometimes easy to forget that electronic discovery is not just about producing documents to the other side. Electronic discovery is also about finding the exculpatory documents that will help you win the case. Of course, finding the “good” documents is only the first step, you also need to make sure that you can get them into evidence. In this guest column, we discuss various steps that organizations should be taking now, even before litigation starts, to make sure that their electronically stored information (“ESI”) is admissible at trial. As Chief Magistrate Judge Paul Grimm has cautioned, litigants who wait to the eve of trial to start thinking about whether they can get electronic information into evidence, may find that it is already too late. *See Lorraine v. Markel Am. Ins. Co.* (“Lorraine”), 241 F.R.D. 534, 542 (D. Md. 2007).

Taking Care of Your Electronic Evidence

We start with an obvious point. You cannot use what you have not kept. If you want to have evidence to use at trial, the first thing you need to do is preserve it. Efforts to preserve evidence should begin before litigation is even anticipated and be part of a company’s document retention practices. These practices must be well-articulated and documented, so that employees can follow them. Document retention typically works best when it is a collaborative effort among Legal, IT, Human Resources, and business units.

Once litigation is reasonably anticipated, preservation efforts become mandatory and often include the issuance of a document hold. The hold should cover all the myriad forms of ESI and provide employees with explicit instructions for preserving them. *See, e.g., Arteria Prop. Pty Ltd. v. Universal Funding V.T.O., Inc.*, No. 05-4896 (PGS), 2008 WL 4513696 (D.N.J. Oct. 1, 2008) (sanctioning defendant for failing to preserve the content on its website).

How you preserve ESI may determine whether you can use it at trial. As Judge Grimm emphasized, “The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial.” *Lorraine*, 241 F.R.D. at 557-58 (quoting *Am. Express Travel Related Servs. v. Vinhnee (In re Vee Vinhnee)*, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005)). In other words, it pays to engage in proper data management.

Organizations should consider the creation of IT data maps that capture the location of data on a system (by custodian, document type, department or office) and inventories of stored information and logs that reflect hardware or software installations, modifications and upgrades. *In re Vinhnee*, 336 B.R. at 448-49. Records and data stored on a computer can usually be authenticated by evidence that is produced by that computer. *See* FED. R. EVID. 901(b)(9). But, among other things,

Hughes
Critical matters. Critical thinking.®
Hubbard

courts look for proof of the reliability of the particular computer used and the dependability of the business's input procedures.

One challenge is to preserve ESI without altering it. Courts want assurances that parties have used proper procedures for handling the electronic records they seek to admit. Counsel must coordinate closely with IT departments and eDiscovery vendors to ensure that these concerns are met, and that the integrity of the data is not "compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling." MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004). Careful practices include:

Chain of Custody Logs — With respect to the preservation and collection of ESI, all actions done to hardware or images should be documented as part of an electronic chain of custody. Chain of custody logs track how ESI is gathered, analyzed and preserved for production. This means documenting what files were opened, every search and action performed, and the time and date of every step. These logs typically include a description of the forensic acquisition methodology used, minimize susceptibility to attack, and enhance credibility before a judge, particularly where there is an allegation of tampering. *See United States v. Tropeano*, 252 F.3d 653 (2d Cir. 2001); *United States v. Block*, 148 Fed. App'x 904, 910-11 (11th Cir. 2005).

Email Audit Trails — Some view email as the type of ESI that is most easily altered. For this reason, one should be prepared to demonstrate the authenticity of email under a strict standard of scrutiny. For those with an email archive, the archiving software generates a useful authentication tool. This software preserves email and attachments by automatically sweeping them from email servers (*e.g.*, Microsoft Exchange and Lotus Notes) into a central repository. Emails are preserved, indexed or journaled, and retained for a period of time based upon internal policies or external regulatory requirements. Email audit trails generated by email archiving software serve the same function as chain of custody logs: they track access to the email and reduce the risk of spoliation.

Hash codes, Encryption and Digital Signatures — Certain technologies demonstrate the integrity of various forms of ESI over time. Making a forensically sound copy requires a bit for bit copy that generates a digital fingerprint. This fingerprint is called a "hash code" (a unique alphanumeric string that is generated by an algorithm and assigned to a document) and serves as evidence that a document has not been altered since the time of retrieval. This not only preserves the integrity of information in, for example, a spreadsheet, but also helps to identify and distinguish one version of a file from another. This is particularly useful when seeking to demonstrate that a version of a document is the "final" or "legally binding" one. Hash codes are typically generated at the time of collection, and maintained and documented from that time through review, production and, ultimately, presentation at trial.

Encryption and digital signatures also provide some basis of reliability. Essentially, encryption is like a secret key which scrambles file contents making it accessible only to those that have the key. Digital signatures employ the same technology and provide assurances that a "signed" electronic document is reliable. These technologies, however, have limitations because individuals other than the owner of the encryption key may obtain access to them and alter the substance of the document.

Metadata — ESI has its own "built-in" evidence that, when handled properly, demonstrates, among other things, that the ESI has not changed since it was preserved. Metadata, or "data about data," is the behind-the-scenes information that describes the history, tracking or management of ESI. Examples of metadata for electronic documents include a file's name, location (directory or path name), format or type, size, and various dates (*e.g.*, creation date, date of last modification, date of last access). Date and time stamps, for example, may be proffered to show that only the author of the document accessed electronic records or that the records have remained intact since the litigation was reasonably anticipated. Other kinds of metadata, *e.g.*, headers, footers, users, edit dates, author, and prior versions of a document, might reveal, for example, the identity of person who is blind copied on an email. *See*,

e.g., *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005).

Federal Rule of Evidence 901(b)(4) permits authentication by “[a]pppearance, contents, substance, internal patterns or other distinctive characteristics, taken in conjunction with circumstances.” Metadata is a good example of a “distinctive characteristic” that can demonstrate, among other things, file ownership, file permissions, creation and modification dates, and other evidence that ties the electronic document to the putative owner and/or custodian.

Note, however, that not all metadata may be seen by the user (size and date); others are hidden or imbedded and may need to be extracted by an expert. Metadata may be easily or inadvertently altered, simply by opening a file or even by saving a document in an effort to preserve it. Knowledgeable IT staff and experienced eDiscovery vendors are therefore critical to a successful preservation process. Further, although a debate exists as to whether metadata must be produced absent a specific request, organizations are well-advised to preserve metadata in case it is needed.

Hearsay

In addition to authenticating ESI, litigants must also think about how they are going to overcome hearsay objections. Defendants typically do this through the business records exception codified in, among other places, Federal Rule of Evidence 803(6). While most courts are willing to recognize ESI as a business record provided that the traditional factors are satisfied, at least one has treated ESI more strictly. In *In re Vee Vinhnee*, 336 B.R. 437 (B.A.P. 9th Cir. 2005), American Express sought to have a debt excepted from discharge in a credit card holder’s bankruptcy proceeding. At trial, American Express tried to introduce monthly credit card statements as business records, but the court rejected the testimony of the company’s records custodian, finding that there needed to be proof of the continuing integrity of the electronic records. *Id.* at 442. The court gave American Express the opportunity to cure the testimonial deficiencies with a post-trial submission and even directed counsel to an evidence treatise on point.

The submission, however, neglected to include what the court was looking for: evidence of American Express’s computer policy and system control procedures, control or access to the relevant database and programs, tracking of changes to the data, backup practices, and other assurances of the continuing integrity of their records. The trial court dismissed the case for failure to meet this additional foundational requirement, *see id.*, and the Bankruptcy Appellate Panel upheld the court’s ruling.

Vinhnee may be an exceptional case, but careful litigants will nevertheless prepare to meet a strict standard. This may mean proffering evidence beyond what is needed to meet the basic elements of Fed. R. Evid. 803(6) and providing adequate assurances that the electronic record is what it purports to be. It may also mean designating an appropriate records custodian, one who has the requisite substantive knowledge and can testify meaningfully about controls that limit system access, practices that track system changes, and back up systems and audit procedures that demonstrate ongoing system integrity. Vague, conclusory, and unpersuasive testimony may not be sufficient to lay a foundation for electronic business records.

Conclusion

Organizations need to manage electronic documents not only to comply with discovery requirements and avoid possible sanctions, but also to help them defend and win cases. This means identifying key evidence early on, anticipating its use, and preserving it in a manner that minimizes its vulnerability to attack. Although many factors play a role in the admissibility of ESI, Judge Grimm has cautioned that there is no substitute for “thoughtful advance preparation” to avoid the “self-inflicted injury” of failing to make a *prima facie* showing of authenticity during litigation. *Lorraine*, 241 F.R.D. at 542. After all, good facts mean nothing if a judge or jury never hears them.

Published in Law360 on February 24, 2009