



Hearsay and Foundation Issues Affecting Your Use of ESI

By Anthony Carriuolo and Thomas A. Sadaka

Having listened intently to seminars about e-discovery rules and pitfalls, including *Zubulake* and *Morgan Stanley* issues, you and your client have faithfully satisfied your duties to preserve relevant electronically stored information (ESI) as litigation became probable. More recently, you have worked through discovery conferences with opposing counsel and the court, and have produced your ESI (or discovered your opponent's ESI) in a cost-effective and fruitful way. Now what? How do you actually use this stuff as evidence?

This article will highlight some of the evidentiary issues that litigators must address when seeking to use ESI as proof. Established hearsay rules (and exceptions), as well as basic foundational matters, must be meshed with ever-evolving technologies and the myriad ways businesses collect, store, and use ESI. The evidentiary issues presented by ESI are as boundless as the information itself, but certain general principles should prove instructive.

Laying a Proper Foundation

To establish a proper foundation for the admission of ESI, you need to know the root of the data being offered. How was the ESI originally created? To what extent does it contain computer-generated data, as opposed to computer-stored data? What opportunities have existed for the data to be corrupted or manipulated—how trustworthy are the data you are offering (and the systems producing or storing it)?

To lay a proper foundation for the admission of ESI, you must enable the court to understand many facts establishing what these data are: how they were created and how they have been stored; who has been responsible for maintaining the integrity of the data and how the data have been maintained; how the specific type of evidence you wish to admit compares with the underlying data it purports to reflect; and whether the ESI you seek to admit satisfies the basic tenets of trustworthiness, accuracy, relevancy, and probative value.

Federal Rule of Evidence 901 generally requires a proponent of evidence to establish its authenticity; that is, that the evidence is what the proponent claims it to be. Because of the many forms in which ESI is maintained and stored, and in which it may be presented to the court, you must be prepared to demonstrate every step through which the evidence being offered has been created—in effect, its genealogy. In some respects, the presentation necessary to introduce ESI is similar to that useful to establish your right to use summaries under Federal Rule of Evidence 1006; that is, a showing

that the item being offered accurately represents or illustrates the source information it purports to reflect in summary fashion. Of course, the original source data must be made available under the normal use of summaries. This, however, may be a formidable hurdle to overcome when the underlying source data comprise many gigabytes of information in many forms. Indeed, our ability to illustrate or calculate millions of bits of data through more digestible computerized forms necessarily prompts us (and hopefully the court) to accept more easily the notion that legitimate evidentiary concerns may be satisfied without delving deep into the depths of data creation. Yet, how deep is deep enough to protect against the introduction of manipulated, misleading, or incomplete ESI?

Obviously, the answer will depend a great deal on the specific nature of the ESI being offered into evidence and the particular means by which the data were created or input, including the extent to which human involvement may have influenced the data.

Knowing Your Data and Its Level of Human Contact

The task of authenticating and admitting ESI is complicated further by the fact that some ESI is actually generated by operation of computer programs (computer-generated records). Examples of computer-generated records include automated records of landline or mobile phone calls, activity records generated by electronic toll collection devices, Internet service provider activity logs, and other records of basic activities that are electronically created without human intervention. Authentication questions for computer-generated records would focus on the reliability of the processing and output functions of the program that has created the record. Note that Federal Rule of Evidence 901(b)(9) permits authentication in these instances by offering “[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”

On the other hand, you may want to introduce human-created information that has simply been stored in electronic form (computer-stored records). This evidence could include electronic forms of telephone messages, customer surveys, investigative reports, emails, correspondence, memorandums, and other word-processing files. Primary authentication questions for computer-stored records focus on identifying the author of the record and showing that the record has not undergone significant change in any respect material to its probative value.

Some records may contain a combination of computer-stored and computer-generated evidence. For example, an Excel spreadsheet contains both the input data that originated from a person (numbers as well as formulas developed and input to run the numbers) and the output of the calculations run by the computer program itself once data and formulas have been entered.

Overcoming Objections with Foundational Proof

If any of these foundational questions are raised with any vigor, the proponent of the electronic evidence must be prepared to present witnesses to overcome each element. You and your client should seek skilled witnesses who are thoroughly familiar with the client's relevant digital hardware and software and who are able to communicate, with a high degree of confidence, that the digital data customarily generated by the client's systems are trustworthy. Your presentation on foundation should include proof that the client's employees regularly and materially rely upon the accuracy and completeness of the digital data when performing important tasks and making decisions for the client. This is especially true if a significant portion of the digital data emanated from employees inputting numerical figures or narratives. Your presentation checklist should include the following inquiries:

- Who handled the evidence from its genesis to its presentation (or production through discovery)?
- What are the names and job functions of all persons who had control of the digital evidence?
- How was the digital evidence collected and stored? What tools and methods were used to collect the data? What safeguards were implemented to control slanted or incorrect input of raw data (especially if the digital data were intended to compile hearsay information)?
- Who had access to the digital evidence after it was collected? How were the raw data manipulated or formatted for future analysis and presentation? What safeguards were implemented to protect the integrity of the underlying data? Can each user's editing activities within the digital evidence (metadata) be tracked and examined? Was the information password-protected or encrypted?
- Could the raw data be produced separately to demonstrate the ability to rerun analyses, to counter any suggestions that the end product is biased, incomplete, or not trustworthy?
- What hardware, software, operating systems, and system configurations were used to gather, initially compile, or ultimately analyze or manipulate the data?

You should remain mindful of the need to present witnesses from various departments to provide the court a firm understanding of how the digital data are created, stored, manipulated, and regularly used. For instance, call your in-house IT expert as a witness to discuss the technical aspects of computer hardware, programs, and the ability to trace user access; introduce testimony from your

client's accounting, marketing, or sales forces to discuss the means by which data are regularly input, manipulated, and used in the conduct of business. Finally, you should evaluate whether the data and programs in play warrant recourse to external experts to corroborate your client's views on the sanctity of its digital records or on any unique aspects of programming that would ease the trier of fact's acceptance of your evidence as complete, accurate, and possessing integrity upon which the court may rely in resolving issues of fact.

Addressing the Critical Objections to Admission

To the greatest extent possible, seek stipulations as to certain basic matters affecting the digital data being offered, including general technical issues that are not genuinely in dispute. You should focus on the pivotal technical concerns the trier of fact is expected to harbor when considering whether to accept your digital data as credible "facts"; spend your time allaying those fears instead of presenting a technical tutorial that may create more questions than answers.

Begin to identify objections to the admission of digital evidence as early in the pretrial process as possible.

You should use discovery conferences, motions in limine, and other pretrial methods to ferret out objections to the digital evidence that he or she intends to offer, and identify persuasive proof to overcome those objections forcefully. Offer up representative samplings from your digital evidence to illustrate clearly the life of your digital data; walk the court through a "day in the life" of the data you wish to present in electronic form. You should avoid addressing complex technical evidence issues for the first time at trial. Begin to identify objections to the admission of digital evidence as early in the pretrial process as possible.

Dealing with Multiple Layers of Hearsay

The hearsay exception most commonly applied to computerized records is the business records exception. To establish the foundation for this exception, the proponent of the evidence should be prepared to show that the computer equipment (hardware and software) on which it was stored is recognized as standard in the field; the data were entered in the regular course of business at or reasonably near the time of the occurrence of the event recorded;

the sources on which the records were based, as well as the method and time of preparation, indicate that the records are trustworthy and their admission is justified.

The rationale for the hearsay rule does not apply to evidence generated directly by a machine.

This foundation for admission may be established through the testimony of the custodian of the record or a person who is familiar with the methods and systems through which it was prepared, even if that person does not have personal knowledge of the underlying facts contained in the record. Supportive evidence might include company reliance on the data, protection of the accuracy of data entry, prevention of loss or alteration of the data after entry, and the provision for the integrity of data output.

The admission of digital records might involve two levels of hearsay analysis. The act of data entry is itself an out-of-court “statement” under Federal Rule of Evidence 801(a), but the result

is usually the record kept in the regular course of business, which ought to be admissible under Federal Rule of Evidence 803(6). In addition, the underlying data entered may contain hearsay “statements” that must also qualify under a hearsay exception.

A record generated by a computer program is not properly regarded as hearsay; it is neither “an oral or written assertion” nor “nonverbal conduct of a person if it is intended as an assertion.” The rationale for the hearsay rule—the preference for testing the trustworthiness of human assertions through in-court testimony subject to cross-examination and observation of witness demeanor by the trier of fact—does not apply to evidence generated directly by a machine.

Paying Attention to Details

With the growing use of ESI as relevant evidence in dispute resolution, trial counsel need to be keenly aware of the multiple, and multilayered, issues affecting its admissibility. To present effective proof supporting the foundation, authenticity, and overall admissibility of ESI, counsel must drill down to the root of the digital evidence to be presented and should be prepared to walk the trier of fact carefully through the process in which raw data have been transformed into the specific digital evidence sought to be admitted. ■

Anthony Carriuolo is a partner and Thomas A. Sadaka is an associate with Berger Singerman.



**Powerful Ideas,
*Straight from the Source.***

If you're like most lawyers, time is at a premium. While in-person CLE programs are great for networking, it can be difficult to make time to travel to a seminar.

With the Litigation Series Teleconferences, you get the programming you need, wherever you are. Featuring nationally known lawyers and judges, the programs offer a lively and balanced examination of the issues litigators care about. It's as easy as picking up the phone. No plane ticket required.

Get connected today at
www.abanet.org/litigation/teleconferences/

 **SECTION of LITIGATION**
AMERICAN BAR ASSOCIATION