IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Commentary_on_ESI_Evidence_and_Admissibility

THE SEDONA CONFERENCE® WORKING GROUP SERIES

WGS℠

THE SEDONA CONFERENCE® COMMENTARY ON ESI EVIDENCE & ADMISSIBILITY

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

MARCH 2008

The Sedona Conference®

The Sedona Conference Commentary on ESI Evidence & Admissibility

Editorial Committee*
Kevin F. Brady
Conor R. Crowley
Paul F. Doyle
Maureen E. O'Neill
James D. Shook
Jack M. Williams

* This Commentary was the subject of dialogue at two Working Group 1 Meetings, and many Working Groups Members submitted comments and edits as well. Thanks go to all who participated in the dialogue that led to this Commentary.
In addition, we thank all of our Working Group Series℠ Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors just click on the "Sponsors" Navigation bar on the hompage of our website.

Introduction

During the last decade, culminating with the adoption of significant amendments to the Federal Rules of Civil Procedure ("FRCP") on December 1, 2006, the legal community has expended significant energy and focus on electronic data. A main focus has been on whether and under what circumstances a litigant must provide such data – known more formally as electronically stored information or "ESI" – to an adverse party.

While there are still significant issues to resolve with the amended FRCP and electronic discovery, the legal community is also grappling with whether and how ESI, once produced, can actually be authenticated and used as evidence at trial or in motion practice. As succinctly noted by Judge Grimm in a recent, leading case on the subject:

> [C]onsidering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.
>
> *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 538 (D. Md. 2007).

This commentary focuses specifically on that concern, and is divided into three parts: Part I is a brief survey of the applicability and application of existing evidentiary rules and case law addressing the same. Part II addresses new issues and pitfalls that are looming on the horizon. Part III provides practical guidance on the use of ESI in depositions and in court.

I. A Survey of the Applicability of Existing Rules & Caselaw

A. Early Focus on Authentication and E-Evidentiary Issues

While there are only a few Federal cases providing guidance in this area[1], Judge Grimm's discussion in *Lorraine* makes it clear that parties should start to think about evidentiary issues much earlier than was the practice when dealing only with hard copy evidentiary materials. Consideration should be given to how potential e-evidence is handled by records management programs, and parties should be mindful of authentication possibilities throughout the discovery process. For example, under the pretrial disclosure provisions of Rule 26(a)(3), a party has 14 days to object to the admissibility of an opponent's proposed documents of other trial exhibits, and the failure to do so results in a waiver. Additionally, given the extent to which summary judgment has replaced trial as a procedure for resolving legal disputes, parties should be prepared to deal with evidentiary issues at the summary judgment stage.

B. Summary Judgment Motions and E-Evidentiary Hurdles

Summary judgment is a critical stage in any litigation, and is likely the first time that the issues of evidence admissibility, including authenticity, will be considered because the court is only allowed to consider evidence that is admissible. *Celotex Corp. v. Catrett,* 477 U.S. 317, 322, 106 S.Ct. 2548, 2552 (1986).

As explained in *Lorraine*, unsworn, unauthenticated documents cannot be considered by the Court in a motion for summary judgment because the Court may only consider evidence that would be admissible at trial.[2] Judge Grimm also discussed in great detail the evidence rules:

> . . . that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.

Lorraine at 538.

---

[1] See *Lorraine*; *U.S. v. Safavian,* 435 F. Supp. 2d 36 (D.D.C. 2006); and *In Re Vee Vinhnee,* 336 B.R. 437 (9th Cir. BAP (Cal.) 2005).

[2] The Court in *Celotex* noted that under FRCP 56(e) a party can oppose summary judgment using any of the kinds of evidentiary materials identified in Rule 56(c), except for the pleadings themselves, and it is from that list (which includes affidavits) that one would normally expect the nonmoving party to make that showing. 477 U.S. at 324. However, that is not always the case. Affidavits, by themselves, are hearsay and do not constitute admissible evidence unless a live witness would testify as to the content of the affidavit thereby making that evidence admissible for summary judgment purposes. If the content of the affidavit would not be admissible if it is offered into evidence at trial by a live witness, then it is not considered admissible evidence for summary judgment purposes notwithstanding the fact that it is in an acceptable form for Rule 56(c) purposes.

C. Authentication Tools – F.R.E. 104, 901 AND 902

There is a complex interplay between "preliminary rulings" on admissibility, governed by Rules 104(a), (b), and the authenticity determination, governed by Rules 901 and 902. As explained in *Lorraine*, under Rule 104(a), the court, not the fact finder, makes the admissibility determination, and in making that determination it is not bound by the restrictions of the Rules of Evidence, except those concerning privileges. *Id.* at 539. Rule 104(a) governs the admissibility of matters such as whether an expert is qualified and, if so, whether his or her opinions are admissible; existence of privilege; and whether evidence is hearsay, and, if so, if any recognized exception applies. *Id.*

On the other hand, the authenticity of ESI and other evidence is governed by Rule 104(b), which affords the court a much narrower role. The court addresses only a threshold question of law: does the proponent's evidence have sufficient probative value to sustain a rational jury finding that the evidence is what the proponent claims it to be? The fact finder makes the ultimate determination of whether the evidence is authentic. For example, if an e-mail is offered into evidence, the determination of whether it is authentic would be for the jury to decide under 104(b), and the facts that they consider in making that determination must be admissible evidence. *Id.* at 540.

The methods a proponent uses to authenticate ESI, i.e., to show that it is what the proponent claims, are set forth in Rules 901 and 902. Just as with "hard copy" evidence, a party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. Id. at 542. This is not a particularly high barrier to overcome. For example, in *United States v. Safavian,* 435 F. Supp. 36 (D.D.C. 2006) the court analyzed the admissibility of e-mail, noting, "[t]he question for the court under Rule 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is....' The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so." *Id.* at 38.

While courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication of "hard copy" documents, they have been quick to reject calls to abandon the existing rules of evidence when doing so. In *In Re Vee Vinhnee,* 336 B.R. 437 (9th Cir. BAP (Cal.) 2005), the court addressed the authentication of electronically stored business records. It observed "[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained . . . ." *Id.* at 444. However, it quickly noted "[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records. Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be." *Id.* It is important to note that the methods for authentication listed in FRE 901 and 902 are non-exhaustive and can be used in combination with each other, and courts have pointed out particular provisions of 901 and 902 that are appropriate or most useful for specific types of ESI.

D. Various Types of ESI Require Different Approaches

All ESI evidence shares certain common characteristics, but some ESI may require a different approach to authentication. The creator of certain types of ESI may be unidentifiable; the ESI may be stored in different types of systems and with different security; and the ESI may contain clues about its history and whereabouts or be completely lacking in provenance. It is thus useful to quickly survey a few representative types.

1. Paper Copies

Both *In Re Vee Vinhnee* and *Lorraine* contain numerous points of comparison between ESI and paper-based record systems in resolving their respective issues. While comparisons to the familiar world of paper-based, tangible evidence are a useful starting point in many legal analyses, it is important to note some of the key differences between the two systems.

With paper-based record systems, the mechanics of creating, storing, managing, organizing, controlling and securing records and the systems that maintain them are generally simple and easily understood. Control largely depends on physical access to the records, which are basically stable and durable; one would need to be physically present to manipulate, mutilate or destroy a paper-based record. Moreover, manipulation or mutilation of documents has the potential for leaving indications of the tampering. Control systems can be designed to take advantage of physical realities such as the contiguous nature of the environment in which the records persisted, including known points of ingress and egress, singularity (uniqueness, originality, and the fact that a paper-based record cannot simultaneously be physically present in more than one location at the same time). Further, a physical or paper-based record cannot be accessed and used simultaneously by multiple people without those people also being physically present and aware that access and use are shared.

This is not the case with ESI, particularly with regard to the issues of controlling and securing records, and access to ESI is not naturally constrained. In fact, most computers are members of networks (or are intermittently on and off networks in the case of laptops), and, to further complicate matters, these networks themselves generally are inter-networked. With computers, control and security are such specialized subjects that even experts in the general subject of computer science defer to more specialized experts.

2. Email

Emails deserve special attention at every level -- retention, preservation, collection, production, and metadata – because of the evidentiary challenges presented. Emails present especially interesting evidentiary challenges because email systems are inherently insecure and unreliable, but there are many ways in which email evidence may be authenticated: (i) 901(b)(1) (person with personal knowledge); (ii) 901(b)(3) (expert testimony or comparison with authenticated exemplar); (iii) 901(b)(4) (distinctive characteristics, including circumstantial evidence); (iv) 902(7) (trade inscriptions); and (v) 902(11) (certified copies of business record). *Lorraine* at 555.

Rule 902(11) is particularly helpful in establishing the foundation elements for a business record without the need to call a sponsoring witness to authenticate the document and establish the elements of the hearsay exception. Rule 902(11) permits the self-authentication of a business record by showing that the original or

a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record: (a) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (b) was kept in the course of the regularly conducted activity; and (c) was made by the regularly conducted activity as a regular practice. *Id.* at 571.

Because the elements for Rules 902(11) and 803(6) are essentially the same, they frequently are analyzed together when Rule 902(11) is the proffered means by which a party seeks to admit a business record. Id. at 572. (citing *In re Vee Vinhee,* 336 B.R. at 446, and *Rambus*, 348 F. Supp. 2d at 701) (holding that analysis of Rules 803(6) and 902(11) go " hand in hand," and identifying the following requirements for authentication under 902(11)(1): a qualified custodian or other person having personal knowledge makes the authenticating declaration, who must have "sufficient knowledge of the record-keeping system and the creation of the contested record to establish their trustworthiness"; (2) the declaration must establish that the record was made at or near the time of the occurrence or matters set forth in the document by someone with personal knowledge of these matters or from information provided by someone with personal knowledge thereof; (3) the declaration must show that the record is kept in the course of the regularly conducted activity of the business, and the "mere presence of a document ... in the retained file of a business entity do[es] not by itself qualify as a record of a regularly conducted activity"; and (4) the declaration must establish that it is the regular practice of the business to keep records of a regularly conducted activity of the business, and "it is not enough if it is the regular practice of an employee to maintain the record of the regularly conducted activity . . . it must be the regular practice of the business entity to do so" -- i.e. it is at the direction of the company that the employee maintains the record). *Lorraine* at 572.

With respect to the "personal knowledge" component of Rule 803(6) (that there be personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant), it is relatively simple to prove personal knowledge if the maker of the business record, the e-mail, has the requisite personal knowledge. However, in many instances, the e-mail contains information from a source outside the business of the maker of the business record and that presents special evidentiary problems. In Lorraine, the court noted that the majority view for meeting the requirements of the business record exception in that situation is the supplier or source of the information memorialized in the e-mail must have had a business duty to transmit the information to the maker of the record, if the maker, himself or herself, lacks personal knowledge of the facts or events. *See Id.* footnote at 52. (citing Fed. R. Evid. 803(6), advisory committee's note ("Sources of information presented no substantial problem with ordinary business records. All participants, including the observer or participant furnishing the information to be recorded, were acting routinely, under a duty of accuracy, with employer reliance on the result, or in short "in the regular course of business.' If, however, the supplier of the information does not act in the regular course, an essential link is broken; the assurance of accuracy does not extend to the information itself, and the fact that it may be recorded with scrupulous accuracy is of no avail.")).

"However, some courts have held that it may be possible to meet the requirements of the business record exception even if the source of the information had no business duty to provide it to the maker of the record, if the recipient of the information has a business duty to verify the accuracy of the information provided." *Id.* at 571 (citing *Rambus*, 348 F. Supp. 2d at 706-707) (Court noted that ordinarily, when the supplier of the information recorded in the business record does not act in the regular course of the business, an "essential link" in the foundation is broken, but recognized that " [w]hen the source of the information

in the business record is an outsider, the only way to save the record from the jaws of the hearsay exclusion is to establish that the business recipient took precautions to guarantee the accuracy of the given information. Thus, the company must have been able in some way to verify the information provided.") (internal citation omitted)). *Id.*

Finally, special problems with email may arise when an email recipient attempts to authenticate the message on the basis that it was authored by a particular individual whose name appears in the "From" field of the header. For example, email may be susceptible to "spoofing", where the sender of an email uses another's name and makes the message appear to originate from a different location, often through the use of another person's computer.

3. Website Postings, Text Messaging and Chat Room Content

In addressing the evidentiary problems associated with Internet websites, the authentication rules most likely to apply, singly or in combination, are 901(b)(1) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), 90l(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications). *Id*. at 556. Many of the foundational issues encountered when authenticating website evidence apply equally to text messaging and chat room content. *Id.* However, because chat room messages are posted by third parties who use "screen names," it cannot be assumed that the content in question was posted with the knowledge or authority of the website host. *Id.* Obviously, there are foundational requirements that must be met in order to authenticate chat room evidence. The rules most likely to be used to authenticate chat room and text messages are 901(b)(l) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics). *Id.* Other general issues include the actual content of the website at a particular point in time, whether the exhibit or testimony accurately reflect this and, if so, whether the content is attributable to the owner of the site.

4. Computer Stored Records and Databases

The mere fact that information has been created and stored within a computer system does not make that information reliable or authentic. The primary authenticity issue in the context of computer stored records and databases, as identified by the Court in *In Re Vee Vinhnee,* focuses 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. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created . . . . Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.
>
> * * * * *
>
> [For electronic information] [t]he logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded,

> as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

Id. at 444-45.

The methods of authentication most likely to be appropriate for computerized records are 90l(b)(l) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), and 901(b)(9) (system or process capable of producing a reliable result). In addition, in order to meet the heightened demands for authenticating electronic business records, the *Vee Vinhnee* Court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried[3]:

> 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.

Id. at 446-47 (citation omitted).

Although each of these steps seems straightforward, a closer analysis shows that step two can be an extremely difficult condition to meet. The notions of trustworthiness and reliability from the physical, paper-based world, as noted above, do not easily translate to the world of ESI. Indeed, a networked computer may

[3] *See* Edward J. Imwinkelried, Evidentiary Foundations § 4.03[2] (5th ed.2002)

be considered by computer and network security experts to be inherently un-trustworthy, requiring enhancement or upgrading to be considered both trustworthy and reliable.[4] Accordingly, it could be argued that the trustworthiness of a computer should not be presumed, but must be demonstrated by the proponent of ESI.

---

[4] The notion of computers and networks as inherently unreliable is supported by the fact that, during the period 2000–2004, over $40 billion was spent on information security products and services in an attempt to secure computers and networks. In 2007 alone, it is estimated that $38 billion was spent on information security products and services. And in spite of this massive effort and expenditure to secure our systems, computer and network security cannot be guaranteed. Further, experts estimate that 5-20% of all computers in use today are ultimately under the control (remotely) of nefarious parties unbeknownst to the systems' legitimate owners and users. *State of Security*, Peter Kuper, Morgan Stanley, published by the IEEE Computer Society, 1540-7993/05/$20.00 © 2005 IEEE/IEEE Security & Privacy.

II. Anticipating New ESI Evidentiary Issues

There is an old adage that in life, the only thing we can be certain of is change, and with respect to ESI, we can be assured that new types of ESI will develop along with new challenges to their use in legal matters. The inherent characteristics of data and systems make it increasingly difficult to authenticate and manage all types of data for litigation purposes. "There is no 'one size fits all' approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that is often new to many judges."[5]

It is impossible to foresee exactly where technology will take us in the coming years, or how changes to technology will create new ESI challenges. However, we can anticipate challenges in at least five areas: (A) determining the owner/creator of ESI; (B) understanding the limits of technology in authentication; (C) analyzing threats to the integrity of ESI; (D) dealing with the sheer volume of ESI; and (E) identifying the custodian and qualifying the custodian for testimony.

A. Determining the Owner / Creator of ESI

As systems grow more interconnected and complex, determining the actual owner or creator of ESI will also become more difficult. Even now, certain ESI may be created by aggregating data from various sources, with various owners, making authentication an extremely difficult task. However, under FRE 803(6), there is a need for testimony from a custodian or other qualified witness, able to testify as to the source of the information, business circumstances associated with the record's creation and the degree of regularity of the business practice and the record making and maintaining of records. Thus it becomes a threshold issue to determine who – or what – is the creator (or creators) of content so that a determination of authenticity can proceed. There are several issues to consider.

1. Individuals

As with paper documents, many electronic documents are created by a single person. However, after the initial creation, those documents may be passed to others via email, network shares, collaborative environments, USB drives, etc. Those individuals may in turn make minor or major modifications and then store these documents on their own devices, where they may again come under the same cycle. Under these circumstances, determining the "owner" or creator of a document can be problematic.

At a minimum, it is important to be aware that the documents and file systems can provide misleading information. Many electronic documents maintain "metadata", or data about data, within the file itself. In Word, for example, some of this metadata can commonly be found in the "Properties" option which includes an "Author" field. Generally this field is populated upon the initial creation of a document, but many documents build upon prior versions – or may just copy the formatting of a document – and this field is generally not changed after the initial creation. Further, the "Author" field (and other fields) can very easily be changed by a user. As such, in certain cases it may be a useful piece of information in determining an author of a document, but is obviously not a trustworthy indicator. Many other applications have similar types of metadata. As storage of ESI becomes more ubiquitous and more portable, this issue will become more difficult to resolve.

[5] *Lorraine* at 544, quoting Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997).

The question may arise as to whether metadata constitutes hearsay, or even hearsay within hearsay, since metadata is typically embedded within a distinguishable electronic file or other electronically stored information. In order to answer that question we need to be specific about what we mean by metadata. Metadata consists of both system metadata and application metadata. Examples of system metadata include a file's name, location, format and the dates on which a file was created, modified and accessed. System metadata thus consists of information generated by a computer without human input. Application metadata include spreadsheet formulae, and comments or redline changes in word processing documents, and thus is the result of human input.

System metadata does not constitute "hearsay," at least not under the Federal Rules of Evidence, because system metadata is generated by a computer without human assistance. The reason is that under the Federal Rules of Evidence "hearsay", by definition, requires human input. Under Rule 801(c), "hearsay" is defined 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." Rule 801(a) defines a statement as "an oral or written assertion . . . of a person, if it is intended by the person as an assertion" and Rule 801(d) defines a "declarant" as "a person who makes a statement." Thus, the Rule requires a "person" to make a "statement" or to be a "declarant." On the other hand, application metadata, which involves human assistance/input, may constitute hearsay, just as any other "statement" made by a human being.

At least one federal appeals court has determined that system metadata is not hearsay for this reason. In *United States v. Hamilton,* 413 F. 3d 1138 (10th Cir. 2005), a criminal case involving Internet pornography, the district court admitted computer generated "header" information (screen name, subject matter of posting, date images when posting, and IP address) over defendant's hearsay objection. The Tenth Circuit Court of Appeals upheld the trial court's determination that metadata was not hearsay and noted:

> [T]he header information that accompanied each pornographic image is not hearsay. Of primary importance to this rule is the uncontroverted fact that the header information was automatically generated by the computer hosting the newsgroup each time Hamilton uploaded a pornographic image to the newsgroup. In other words, the header information was generated instantaneously by the computer without the assistance or input of a person. As concluded by the district court, this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition of "hearsay." In particular, there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801.

Hamilton, 413 F. 3d at 1142; *see also, United States v. Khorozian,* 333 F. 3d 498, 506 (3d Cir. 2003) (concluding that header information automatically generated by fax machine was not hearsay because "nothing 'said' by a machine . . . is hearsay.") (internal quotations omitted).

2. Shared Collaborative Environments

Collaborative environments, which are quickly spreading through corporate workplaces, present significant issues regarding ownership and creation. In a collaborative environment, multiple users are able to access, modify, store and add information to a common area. Sometimes strict controls track and retain information on who has accessed the document and what changes were made; frequently they do not. Therefore, a document contained in a collaborative environment could have been authored by any one (or all) of the persons who have access to that document. Alternatively one person – perhaps not even listed as having access to the environment – could sabotage one of the documents through deletion, creation of a new fake document or some other method.

The use of collaborative environments is continuing to grow, especially with the fast adoption rate of Microsoft's Sharepoint and similar products; and the skyrocketing usage of wikis and blogs. A wiki is software that allows users to freely create and edit Web page content.[6] A blog is essentially an online journal for public consumption that is usually edited by a single person, but which frequently can be accessed by more than one person. Both wikis and blogs are designed to be easily edited, with prior versions not available online once they are revised (although configurations can be set to retain content through an established number of revisions).

The issues with such technologies are illustrated through issues faced by Wikipedia, a well-known wiki-based encyclopedia – or as Wikipedia prefers, "the free encyclopedia that anyone can edit." Undoubtedly due to its open nature, Wikipedia boasts "over 2,176,000 articles consisting of over 946,000,000 words" and is one of the top-ten visited sites on the Internet.[7] However, the very thing that makes it so powerful – its open nature -- makes its reliability and authenticity questionable at times.[8]

3. System-Created Documents

Another issue arises when a system, instead of an individual, is the creator/owner of a document or file. This frequently occurs when logs of certain activity are automatically created by an application or operating system. For example, a proxy may maintain logs of Internet websites accessed by employees. The authenticity and reliability of data created in this manner is based largely upon the configuration and operation of the underlying systems. In some cases, knowledge of where and how such automatically generated data is created may be known only to the programmer(s) who developed the software – and that information may not be available.

The popularity of Open Source software may both increase the prevalence of authenticity reliability issues and make these issues technically easier to resolve, albeit with a substantial investment of resources. With Open Source, the underlying computer instructions, and/or the "source code," are available to any interested party. This is in stark contrast to the normal practice of most for-profit software companies, who typically preserve their source code as a trade secret. In systems where source code is unavailable, it may be extremely

[6] "What is Wiki", wiki.org/wiki.cgi?WhatIsWiki, last accessed February 8, 2008. *See also*, The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Second Edition), p. 54: "Wiki: A collaborative website that allows visitors to add, remove, and edit content."
[7] http://en.wikipedia.org/wiki/Wikipedia. Last accessed January 15, 2008.
[8] *Id.*

difficult or impossible to provide foundational evidence showing how and where data was created. In Open Source systems, that data is available, but may require a substantial investment of time to have someone with sufficient skill and knowledge determine the answer.

4. Aggregated Documents

Other programs may aggregate information from different sources, reporting the information in a summary fashion or perhaps adding additional processing to the data before its display. For example, a dashboard in a corporate Intranet may pull data from several different sources, some user-created, others system generated, process those inputs in some manner pre-defined by the company (and its programmers) and display the results in a useful manner.

Determining the owner of such a document is likely impossible, or at least time-intensive and expensive. In many cases, this problem can be exacerbated because some, or much, of the ESI may be drawn from an independent third-party. The content contained in a single document or file may therefore be drawn from many different sources, some of which may each be human or machine-based, and others obtained from a third-party through a feed which could, in turn, have its roots from a person or another machine process. The proponent of the document may have little or no ability to determine the author of each idea or paragraph. To what extent will the proponent be responsible for authenticating the information that it received if it intends to introduce a document at trial? And conversely, will it be permitted to challenge that information if it seeks to prevent a document from being entered into evidence? While some of these issues may be resolved by permitting the evidence to be entered with its weight determined by the jury considering these factors, guidance in this area will be difficult.

B. Understanding the Limits of Technology

Given the complexity of the electronic environment, litigants and the courts undoubtedly will turn to technology for assistance in establishing authenticity. Although technology can provide many tools to assist in this process, it is important to understand these tools and their potential role in the authentication process, as well as their limitations.

1. Hashing

A hash algorithm takes a file as input and calculates a unique identifier for that file called a "hash value."[9] Any modification to the file – even changing a single bit out of ten gigabytes – will result in a completely different hash value, indicating that the file has been changed.

---

[9] Losey, Ralph. "Hash: The New Bates Stamp," *Journal of Technology and Law Policy*, Vol

However, hashing is not a test for authenticity in its own right. Rather, hashing can be a means of efficiently determining whether two files are exact duplicates of each other, or whether a single file has been altered. The reliability of hashing depends on a trustworthy reference, so either the subject file or the copy (or its hash value) must be preserved in a way that assures that there has been no tampering with the reference. The main risks or threats to this process are unauthorized access, trusted insider behavior and/or collusion. In particular, a trusted insider, such as an administrator with significant authority to modify a system and its security settings, could make critical changes leaving barely a trace in her wake or none at all.

2. System metadata

Metadata can be another useful checkpoint for determining authenticity. For example, email messages generally contain a substantial amount of metadata information, including a unique message ID as well as information on the unique Internet locations (IP addresses) where the message originated and was handled along the way to its destination.

Similarly, operating system metadata can be a useful tool. Most operating systems maintain information about individual files – the dates that a file was created, last modified and last accessed. For example, in a case where an individual claims that it did not create a document until July 1, but the system metadata shows that the document was created on May 1, this data may be helpful.

However, metadata can be unreliable and is usually subject to manipulation and non-obvious deletion. A moderately sophisticated user may be able to manipulate system dates, and although traces of this manipulation may be left behind, detecting such traces can be extremely difficult and expensive, or simply impossible. Worse, use of files after the fact, such as an investigator opening a file for review, can modify metadata and make it useless or misleading for authenticity purposes. Accordingly, careful attention should be paid to the methods used to authenticate metadata.

3. Encryption/digital signatures

The use of encryption[10] and digital signatures[11] can also provide a basis for trust. At a simple level, encryption uses a secret key to scramble the contents of a file so that only those with access to the key may read the file. A digital signature uses the same technology to enable a party to use its secret key to indicate that it has "signed" an electronic document. Well-established products enable these processes to work fairly seamlessly, although managing the keys used for encryption can become an issue, especially at an enterprise level.[12]

Using these technologies, it is possible to assert that a person signing an electronic document has viewed and approved the document, much as someone would indicate their acceptance of a document (or indicate their authorship of a letter) by signing their name in ink. In legal circles this is commonly referred to as "non-repudiation."

---

[10] "Encryption: A procedure that renders the contents of a message or file scrambled or unintelligible to anyone not authorized to read it." The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Second Edition), p. 19.

[11] "Digital Signature: A way to ensure the identity of the sender, utilizing public key cryptography and working in conjunction with certificates." The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Second Edition), p. 15.

[12] For example, losing access to a key in a properly implemented encryption system would render a message or file lost and completely unreadable. Thus, a loss of such keys during litigation could lead to a spoliation concern.

However, a digital signature actually indicates something slightly different – that someone with access to the key has signed the document. Keys can be stolen or borrowed (copied), frequently without the knowledge of the owner of the key. Similarly, one must link a key back to a specific individual, which generally requires an inquiry to the party that issued the key, and an assessment of the veracity of the key issuer. And even assuming a reputable issuer, that party may distribute keys under varying levels of scrutiny --- requiring only an email address at the low end, all the way to requiring a passport or other official identification at the higher end.

For example, it may easily be proven that a key issued to John Smith by KeyCorp was used to sign an important document. However, upon inquiry to KeyCorp, it may be determined that the key was sent via email to JohnSmith@yahoo.com, without any verification of John Smith's identity.

Additionally, there is nothing about a plain digital signature that can be used to prove when it was created. It is possible for a party in control of the digital certificate (cryptographic key) to falsify the value/appearance of time in conjunction with manipulated data and force a signing event that would be technically impossible to identify or distinguish from a legitimate digital signature. In such a scenario, the resulting data/signature combination would be mathematically true but semantically false.[13] However, digital signatures can be used in combination with alternative methods for establishing authenticity.

4. Storage

The simple act of storing ESI within a system does not necessarily render that ESI inviolate for purposes of authenticity. In fact, In Re Vee Vinhnee largely turned on the issue that there was no testimony to establish that ESI placed into storage had not been modified between that time and the trial date.

> The primary authenticity issue . . . 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. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created."[14]

The court further explained that "the focus is on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

Parties relying on storage media to establish that their information has not been changed after being stored can rely upon a variety of technologies. WORM[15] technology can for all practical purposes ensure that information, once written, is not erased. Although originally implemented on optical platters, such storage has become more sophisticated and can be implemented on a variety of electronic storage media, including hard drives with built-in safeguards.[16] Other storage systems can ensure that information, once written, is preserved for a predetermined amount of time, and software can play a role in preserving data from deletion or at minimum reporting that it has been deleted.

[13] ieeexplore.ieee.org, The Digital Signature Paradox, http://ieeexplore.iee.org/xplore/login.jsp?url=iel5/10007/32124/01495999.pdf (last visited February 5, 2008).
[14] *In Re Vee Vinhnee at* 444.
[15] "WORM" is an acronym for "Write once, read many," *See* The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Second Edition), p. 55.
[16] Broker-dealers generally relied upon optical disk to meet the books, records and other communications requirements under Rules 17a-3 and 4. Over time, other electronic systems with built-in safeguards met these requirements and were approved for use by the SEC. 17 CFR Part 241, Release No. 34-47806, "Electronic Storage of Broker-Dealer Records".

However, it is important to understand that these systems have limitations. First, and most important, the act of storing the information does not establish authenticity; the validity of the information depends on the process that placed it there. In other words, if there are not proper processes in place to ensure that the information is valid when written, the fact that the information is properly preserved is meaningless. Second, there are various types of systems and media available, all with differing characteristics on how securely they store the data initially, whether and under what circumstances they permit its manipulation or deletion, and what evidence or logging is left behind to show that such changes occurred. Finally, as more fully discussed below, these systems are not foolproof and can be susceptible to attack.

5. Trusted Time Stamping

Time is already one of the elemental criteria of ordering, management and control. The ability to verifiably establish true and non-alterable time for ESI can significantly improve the ability for self-authentication. Trusted time stamping is the name for a set of mature technical methods to establish the authenticity of the descriptive time value component of ESI. Trusted time stamping is the process of creating a cryptographic binding between a verifiable time value and an associated data-set or record. It is a precise and effective way to make a demonstration of a record's comportment to the condition of timely creation necessary to qualify under FRE 803(6). Trusted time stamping is also a way to demonstrate the unchanged condition of ESI, or conversely to demonstrate change if it has occurred.

6. Computer Forensics

Computer forensics "is the art and science of applying computer science to aid the legal process. Although plenty of science is attributable to computer forensics, most successful investigators possess a nose for investigations and a skill for solving puzzles, which is where the art comes in."[17]

Computer forensics involves the location, examination, identification, collection, preservation and analysis of computer systems and ESI, and often includes the rendering of a qualified expert opinion regarding those systems and ESI. Computer forensics typically involves the employment of specialized and sophisticated computer-based tools to aid in the performance of the various investigation and documentation activities. The downside to the use of a forensics expert includes the cost and time necessary for investigation.

C. Understanding the Threat Landscape

In many ways, the threats of manipulating ESI are similar to the issues (e.g. forgery) faced with paper records. Thus, although we cannot assume that ESI has been changed merely because it could have been changed, being familiar with potential threats and understanding when they may be legitimate concerns is important. And while courts and litigants must be aware of the possibility of these threats, there should be a wariness preventing use of these threats as a casual defense to preclude harmful evidence – the electronic equivalent of "the dog ate my homework."

[17] Chris L.T. Brown, Computer Evidence Collection and Preservation, 2006.

1. Anti-Forensics

Anti-forensics is the employment of sophisticated tools and methods used for the intentional fabrication and/or manipulation of ESI on a computer system intended to thwart forensic examination. In short, anti-forensics is digital forgery.

Manipulation of ESI is likely to grow in the coming years as more tools are created that enable an average user to make sophisticated attacks. "Five years ago, you could count on one hand the number of people who could do a lot of these things . . . Now it's hobby level."[18] Examples of readily available tools include Timestomp and Transmogrify:

> Timestomp . . . targets the core of many forensic investigations—the metadata that logs file information including the times and dates of file creation, modification and access. Forensic investigators poring over compromised systems where Timestomp was used often find files that were created 10 years from now, accessed two years ago and never modified. Transmogrify is similarly wise to the standard procedures of forensic investigators. It allows the attacker to change information in the header of a file, a space normally invisible to the user. Typically, if you changed the extension of a file from, say, .jpg to .doc, the header would still call it a .jpg file and header analysis would raise a red flag that someone had messed with the file. Transmogrify alters the header along with the file extension so that the analysis raises no red flags. The forensic tools see something that always was and remains a .doc file.[19]

Thus, courts and litigants need to become familiar with anti-forensic tools and not become bedazzled by technology, which some fear is occurring. In a paper that appeared in the Journal of Digital Forensic Practice, Vincent Liu and coauthor Eric Van Buskirk flout the U.S. courts' faith in digital forensic evidence. Liu and Van Buskirk cite a litany of cases that established, as one judge put it, computer records' "prima facie aura of reliability." One decision even stated that computer records were "uniquely reliable in that they were computer-generated rather than the result of human entries." Liu and Van Buskirk take exception to this viewpoint. The "unfortunate truth" they conclude, is that the presumption of reliability is unjustified and the justice system is "not sufficiently skeptical of that which is offered up as proof."[20]

2. Interconnectivity

In theory, every system on the Internet can interact with any other system. Sometimes this activity is requested (e.g. requesting a web page from a far-off server); other times it is not and may even be unnoticed by the custodian of the computer (e.g., a direct attack from another computer, virus activity). This level of interconnectivity creates the possibility that an otherwise reliable computer or system could be modified without any physical access.

---

[18] CIO Magazine, May 31, 2007, "How Online Criminals Make Themselves Tough to Find, Near Impossible to Nab" by Scott Berinato.
[19] *Id.*
[20] Eric Van Buskirk and Vincent T. Liu, "Digital Evidence: Challenging the Presumption of Reliability," Jounal of Digital Forensic Practice, 1:19-26 (2006), 25.

3. Enormous Volumes and Various Locations of ESI

One problem we are already encountering, and which is likely to worsen, relates to the vast quantities of information created and stored each day. In 2006, we created, captured and replicated enough digital information to fill all of the books ever created in the world, 3 million times.[21] Similarly, portability and storage capacities continue to grow at very fast rates. Where years ago we might have had access to one computer at work with a small hard drive, many people now have access to two or more computers (including a laptop) with large hard drives, a cell phone with its own independent storage, a PDA, portable USB drives, an iPod or other multi-storage device, online storage capacity, cameras with storage cards, and even automobiles with 40GB hard drives.

Determining how to efficiently deal with this volume of ESI in the litigation process will be a key issue in the coming years. First, the expense of finding, collecting and reviewing the ESI is already used as significant leverage in cases, making the merits of many cases a secondary consideration for the litigant. And this problem is worsening, at least in terms of the volume and sources of ESI. Second, many well-meaning litigants are unable to meet their ESI preservation obligations, despite their best efforts, adversely impacting their ability to litigate the issues. Third, it may be impossible for many companies to enforce litigation holds, to the strict requirement of the obligation, on decentralized devices that are under user control.

III. Practical Guidance on the Use of ESI in Depositions & In Court

In addition to authentication and admissibility issues, the use of ESI in depositions and in court raises novel issues that were not present when evidence was available only in hard copy form.

A. Use of ESI in Native/Live Format vs. Static Format

When introducing ESI as an exhibit in a deposition or in court, the proponent of the evidence must make a decision: should the evidence be offered in its native or "live" format, or should it be reduced to a more static, traditional format?

1. Introducing ESI in Native/Live Format

Using ESI in its native or live format provides the ability to manipulate the data for demonstration purposes. This is particularly important when an issue in the proceedings relates to the output of a program, the way a program functions or the operation of a process. Introducing ESI in its native format also makes visible (or audible) aspects of the information (sight, sound, movement, speed) that are lost when the ESI is reduced to a static format – such as formulas in a spreadsheet and complete addresses in an email message. System and application metadata are also available from native ESI to an extent not generally possible when ESI is in a static form. In addition, it is far easier to test or experiment with data when dealing with native ESI. Finally, although ESI in static format is currently deemed sufficient for purposes of the best evidence rule, this may not be the case with new and exotic forms of ESI.

Although using ESI in native or live format provides clear benefits, there are also a number of disadvantages to using live ESI. Live ESI is not necessarily subject to replication in the precise way it was used in a deposition or in court. Similarly, it may be difficult to make an evidentiary record for the purposes of appeal or other later review when ESI is introduced in native format. ESI in native format also invariably requires far greater on-site resources in terms of hardware and software.

There are a number of relatively simple ways to address authenticity concerns that may be raised when ESI is presented in native format. Screen capture software can record the ESI as it appears on a computer monitor. In depositions, a second video camera can be used to record the ESI appearing on a monitor while the first camera records the deponent. When evidence includes the running of a program or the output of a process, the on-screen depiction of the live event can be captured on video. If speed or sequencing is significant, the video footage can be digitally time-stamped in the same way that videotaped witness testimony can be. For ESI that incorporates sound or video, authenticated copies of the media can be introduced as evidence. Finally, using a printer at a deposition to create a static copy of ESI being shown to the deponent will allow the deponent to authenticate the static copy on the record.

Also, parties may want to consider escrowing a copy of ESI provided on read-only media – or perhaps escrowing the hash value of the media for later verification -- to counter later assertions that the ESI being proffered has been altered after production or is not the ESI that was produced. As courts are generally not willing to take custody of evidence unless it is actually offered in court, the parties will need to find a mutually agreeable technical method or third-party with which the ESI can be escrowed to prevent disputes or quickly resolve them as they arise.

2. Introducing ESI in Static Format

Although not as useful for certain purposes as native format ESI, there are some clear benefits to using a static form of ESI: it is often simpler and cheaper; it is more easily authenticated, replicated, duplicated and distributed. Finally, the hardware and software resources necessary for presenting ESI in native format are not needed to present static ESI.

Of course, this simplicity comes at the cost of eliminating much that may be useful about native ESI. Most system and application metadata is not visible in static images. It is also very difficult to reduce complex databases to static images without losing significant amounts of information. Finally, it is not possible to demonstrate how output is generated, how a program functions or how a process operates when ESI is not in native or live format.

There are a variety of ways in which ESI can be reduced to static form if that form is preferable. The most common method is to electronically "print" the ESI to a flat image file format, such as .tif or .pdf. Some ESI, however, is not well suited to such treatment. If the ESI is viewable on a computer monitor, it can be reduced to static form by printing a screen shot. If necessary, sequential screen shots can be printed as the viewable image changes. Where ESI exists in the form of databases or complex spreadsheets, parties may consider extracting only the pertinent portions of the data and printing those extracts to hard copy. Or, if a witness is being questioned about the structure or organization of data in a database or other compilation, a small sample of the data can be reduced to static form and the witness questioned as to whether, and how, the sample is representative of the contents of the database. For spreadsheets that contain formulas, two copies of the spreadsheet can be converted to a static form: one that hides the formulas and reveals only the output of the formulas in each cell, and one that reveals the formulas, but not their output.

Whether working with ESI in native form or static form, effective use of the information in a manner that permits authentication, and, ultimately, admissibility, requires creativity, flexibility, and the willingness to work cooperatively with opposing counsel. As long as the parties collaborate and commit to focusing on the merits of the case, and not on unwarranted collateral battles about authenticity of ESI, many of the hurdles to authentication and admissibility of evidence can be overcome through agreement and stipulation. And even in those cases where authenticity is a legitimate concern, the parties should seek to discuss and perhaps narrow the scope of the dispute over ESI in good faith. Indeed, the revised federal rules place significant emphasis on such good faith discussions.

B. Practical Tips for Admission of ESI as Evidence

Attached as Appendix A to this paper is a practical guide for working with ESI so that it ultimately will be admissible. The guide includes a checklist of the potential methods of authentication under FRE 901 and 902 that can be used for various types of ESI.

As with all evidentiary material, when working with ESI as tangible evidence, it should be handled with care to ensure that there is a defensible chain of custody. For example, when a hard drive is to be removed for imaging, a photograph of the drive in situ may be taken and the person from whom the drive is obtained can certify the serial number of the drive being removed. At all stages of processing the drive, the persons taking custody of the drive should sign a form acknowledging receipt of the specific drive after verifying its serial number. When the drive is returned, the person from whom the drive was obtained can verify that

the serial number matches their record of the removed drive and be willing to attest that the specific drive removed has been returned.

ESI admissibility issues should be addressed as early as possible. Consideration should be given to incorporating agreements regarding admissibility into production stipulations or submitting these agreements to the court for approval. Given that the difficulties of replicating ESI increase as the degree to which it is static decreases, care should be taken to choose the most replicable form of ESI that provides the necessary probative information (including metadata).

CONCLUSION

Although many questions concerning ESI evidence and authenticity are addressed by the existing body of law in this area, ESI does present some novel issues. In the future, as new forms of ESI emerge, new rules may well be required to address evidence and authenticity questions. This commentary is not designed to provide solutions to all problems, but to encourage members of the judiciary and the bar to ask the necessary questions, and ultimately suggest solutions.

Appendix A

Adminissibility of Electronic Evidence

Admissibility of Electronic Evidence

Paul W. Grimm
Kevin F. Brady

Checklist of Potential Authentication Methods

1 E-mail
- Witness with personal knowledge (901(b)(1))
- Expert testimony or comparison with authenticated examples (901(b)(3))
- Distinctive characteristics including circumstantial evidence (901(b)(4))
- Trade inscriptions (902(7))
- Certified copies of business record (902(11))

2 Internet Website Postings
- Witness with personal knowledge (901(b)(1))
- Expert testimony (901(b)(3))
- Distinctive characteristics (901(b)(4))
- Public records (901(b)(7))
- System or process capable of proving a reliable result (901(b)(9))
- Official publications (902(5))

3 Text Messages and Chat Rooms
- Witness with personal knowledge (901(b)(1))
- Circumstantial evidence of distinctive characteristics (901(b)(4))

4 Computed Stored Records and Data
- Witness with personal knowledge (901(b)(1))
- Expert testimony (901(b)(3))
- Distinctive Characteristics (901(b)(4)
- System or process capable of proving a reliable result (901(b)(9))

5 Computer Animations and Computer Simulations
- Witness with personal knowledge (901(b)(1))
- Expert testimony (901(b)(3))
- System or process capable of proving a reliable result (901(b)(9)

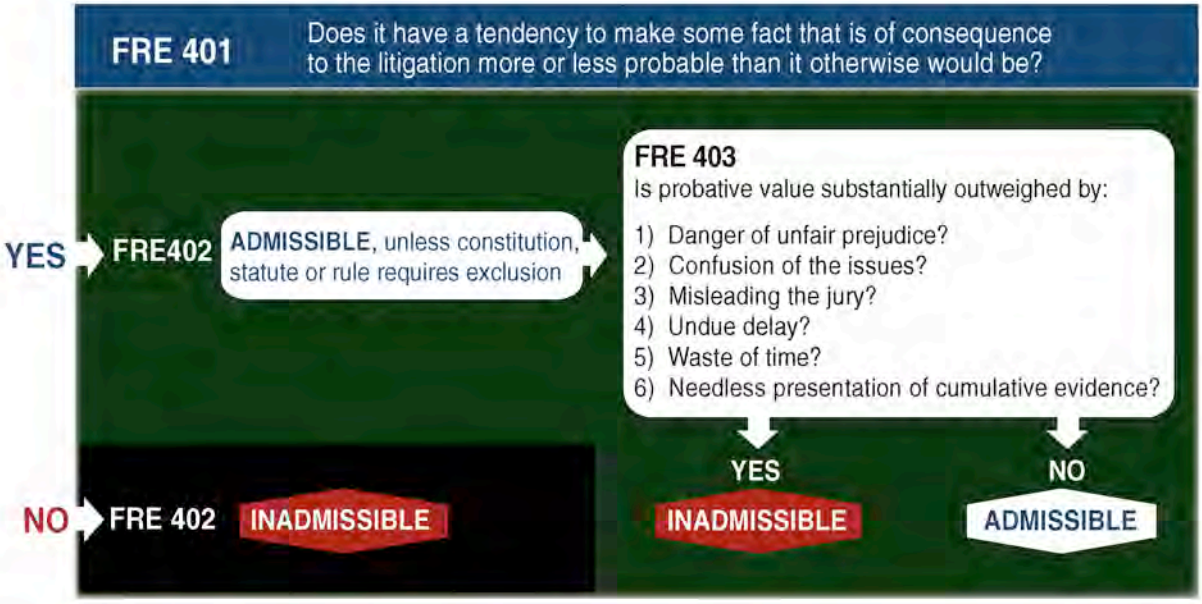
6 Digital Photographs
- Witness with personal knowledge (901(b)(1))
- System or process capable of providing reliable result (901(b)(9)

Design: Mimi Le

1 Preliminary Rulings on Admissibility

- Before evidence goes to jury, judge must determine whether proponent has offered satisfactory foundation from which jury could reasonably find that evidence is authentic (104(a)) (FRE, except for privilege, do not apply)
- Jury determines whether evidence, that is admitted for the jury's consideration, is what the proponent claims it is. Jury determines authenticity (104(b)).

2 Is Evidence Relevant?



3 If Relevant, is it Authentic? FRE 901-902

- **FRE 901(a)** Is the evidence sufficient to support a finding that the matter in question is what proponent claims?

  Determining the degree of foundation required to authenticate electronic evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routines of the computer operation and the ability to test and verify the results.

- **FRE 901(b)**
  Non-exclusive list of examples includes:

  1 Testimony of witness with knowledge;
  3 Comparison by trier or expert witness;
  4 Distinctive characteristics and the like (e-mail address, hash values, "reply" doctrine);
  7 Public records or report; and
  9 Process or system.

- **FRE 902**
  Methods by which information may be authenticated WITHOUT EXTRINSIC EVIDENCE:

- **FRE 902** Does not require sponsoring testimony.

  Three ways to authenticate e-records:
  - 902(5) Official publications
  - 902(7) Trade inscriptions
  - 902(11) Certified domestic records of regularly conducted activity (authenticate business records under FRE 803(6)).

4 Is Evidence Hearsay?

FRE 801 (a) and (b) Is it an out of court statement made by "declarant" (i.e., a person, not a machine); express assertion or nonverbal or verbal conduct w/assertive intent?

YES → **FRE 801(c)**

Is statement being offered to prove the truth of the matter asserted?

- **NO** → **NOT HEARSAY**
  ADMISSIBLE if otherwise relevant examples:
  1. Communicative capacity of declarant
  2. To show effect on hearer
  3. Circumstantial evidence of declarant's state of mind
  4. Verbal acts, parts of acts or utterances of independent legal significance
- **YES** → **HEARSAY**
  NOT ADMISSIBLE w/o exception
  go to no. 5

Are the words being offered for some other reason?

- **NO** → **HEARSAY**
  NOT ADMISSIBLE
  go to no. 5
- **YES** → **NOT HEARSAY**
  ADMISSIBLE

NO → **ADMISSIBLE** as NONHEARSAY (if relevant)

5 If Hearsay, Do Certain Exceptions Apply?

A) Is Declarant testifying at trial?

YES

1. Prior Inconsistent Testimonial Statement? 801(d)(1)(A) (trial, hearing, court proceeding or deposition)
2. Prior Consistent Testimony? 801(d)(1)(B) (rebut express/implied allegation or recent fabrication)
3. Prior Identification? 801(d)(1)(C)

NO → Is declarant unavailable (804(a))

YES

1. Former Testimony? 804(b)(1)
2. Dying Declaration? 804(b)(2)
3. Statement Against Interest? 804(b)(3)
4. Statement re: family history? 804(b)(4)
5. Forfeiture by wrongdoing? 804(b)(6)

NO Go to other exceptions (803, 807)

B) Is it a Statement by Party-Opponent?

YES

1. Individual Admission? 801(d)(2)(A)
2. Adoptive Admission? 801(d)(2)(B)
3. Statements by person authorized by party to make statement? 801(d)(2)(C)
4. Admissions by agents/employees? 801(d)(2)(D)
5. Coconspirator Statements? 801(d)(2)(E)

NO → Go to FRE 803 or 807

C) Should the statement be considered reliable because of other circumstances?

(Not excluded by hearsay rule even though declarant is available as a witness?)

YES

1. Present Sense Impression 803(1)
2. Excited Utterance 803(2)
3. State of Mind Exception 803(3)
4. Statements for Purposes of Medical Diagnosis or Treatment 803(4)
5. Past Recollection Recorded 803(5)
6. Business Records 803(6)
7. Absence of an entry in records kept in the regular course of business 803(7)
8. Public Records or Reports 803(8)
9. Records of Vital Statistics 803(9)
10. Absence of public record or entry 803(10)
11. Records of Documents affecting interest in property 803(14) & (15)
12. Statements in Ancient Documents 803(16)
13. Market Reports, Commercial Publications 803(17)
14. Learned Treatises 803(18)
15. Character Reputation Testimony 803(21)

NO → **INADMISSIBLE**

6 Original Writing Rule - FRE 1001 - 1008

- Is the evidence "original", "duplicate", "writing", "recording" (1001)

- Rule 1002 requires the original to prove the contents of a writing, recording or photograph unless "secondary evidence" (any evidence other than original or duplicative) is admissible. Rules 1004, 1005, 1006, 1007.

- Duplicates are co-extensively admissible as originals unless there is a genuine issue of authenticity of the original or circumstances indicate that it would be unfair to admit duplicate in lieu of original (1003)

- Permits proof of the contents of writing, recording or paragraph by use of "secondary evidence" – any proof of the contents of a writing, recording or photograph other than the original or duplicate (1004) if:

  i. Non-bad faith loss/destruction of original/duplicate
  ii. Inability to subpoena original/duplicate
  iii. Original/duplicate in possession, custody, control of opposing party
  iv. "Collateral record" (i.e., not closely related to controlling issue in case)

- Admission of summary of voluminous books, records or documents (1006)

- Testimony or deposition of party against whom offered or by that party's written admission (FRCP 33, 36) (1007)

- If admissibility depends on the fulfillment of a condition or fact, question of whether condition has been fulfilled is for court to determine under 104(a) (1008)

- But, the issue is for the trier of fact, if it is a question:

  (a) whether they asserted writing ever existed;
  (b) whether another writing, recording or photograph produced at trial is the original; or
  (c) whether other evidence of contents correctly reflects the contents, the issue is for the trier of fact.

7 Practice Tips

1 Be prepared. Start with a defensible and comprehensive records management program.

2 Think strategically about the case and the evidence from the beginning of the case.

3 Memorialize each step of the collection and production process to bolster reliability.

4 Use every opportunity during discovery to authenticate potential evidence.
Examples:

  a) For pretrial disclosures under F.R.C.P. 26(a), you have 14 days to file objections or possible waiver;
  b) Documents produced by opposing party are presumed to be authentic – burden shifts
  c) F.R.C.P. 36 Requests for Admissions
  d) Request stipulation of authenticity from opposing counsel

5 Be prepared to provide the court with enough information to understand the technology issues as they relate to the reliability of the evidence at hand.

6 Be creative and consider whether there are case management tools that might assist the court and the other parties in addressing evidentiary problems concerning some of the more complex issues (such as "dynamic" data in a database or what is a "true and accurate copy" of ESI); and

7 Keep your audience in mind . . . will this be an issue for the judge or the jury? (e.g., Rule 104(a) or (b).

100% recycled and
30% post consumer waste.