

# **MAKING SURE YOU CAN USE THE ESI YOU GET: PRETRIAL CONSIDERATIONS REGARDING AUTHENTICITY AND FOUNDATION OF ESI**

By: Eric S. Eissenstat

In the modern litigation world, a trial lawyer often requests, assimilates, produces and generates vast amounts of computer data, computer models, computer-generated charts and timelines, animations, e-mails, spreadsheets, digital recordings, website materials, instant messages, digital photographs, chat room transcripts, metadata, etc. This information is only useful, however, if the lawyer can get it into evidence.

Much has been written about the new “e-discovery” amendments to the Federal Rules of Civil Procedure. However, there has not been nearly as much attention or literature on the requirements to use and admit ESI at pretrial proceedings (such as summary judgment) or at trial. The Federal Rules of Evidence and the Oklahoma Evidence Code will govern the basic foundational, authenticity and other evidentiary requirements surrounding the introduction of such evidence. While the Federal Rules of Civil Procedure were amended to address specific issues relating to electronically stored information (“ESI”), the Federal Rules of Evidence, for the most part<sup>1</sup>, have remained stagnant.<sup>2</sup> This article will focus on one discrete ESI evidentiary issue – authenticity/foundation – and the best pretrial practices for meeting those requirements.

## **I. INTRODUCTION TO ELECTRONIC EVIDENCE ISSUES**

Digital or computerized evidence is typically in the form of either computerized business records or computer-generated evidence. Computerized business records involve the use of the computer through arranged or compiled objective data, while computer-generated evidence uses the computer to analyze objective input data and generate conclusions based on assumptions contained in the program being run.<sup>3</sup>

With respect to ESI, “no additional authenticating evidence is required just because the records are in computerized form rather than pencil and pen.” Jack B. Weinstein & Margaret A. Berger, *Weinstein’s Federal Evidence* at § 901.08 (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997) (hereinafter referred to as “Weinstein”). Yet, computerized data does raise unique issues concerning accuracy and authenticity.<sup>4</sup> Accuracy can be compromised by incomplete data entry, mistakes in output instructions, programming errors, damaging and contamination of storage media, power outages and equipment malfunctions. (*Id.*) The integrity of data can be impaired in the course of discovery by improper search and retrieval techniques, data conversion or mishandling. (*Id.*) This has led some courts to mandate more stringent authenticity requirements for ESI.<sup>5</sup> Indeed, some courts have expressed skepticism about electronic evidence, finding it “inherently untrustworthy.”<sup>6</sup>

Professor Imwinkelried cautions:

There are many common, comforting myths about digitized evidence. However, we must come to grips with the harsh realities: Electronic

evidence can be modified, it is vulnerable to hackers, the alteration of electronic evidence is difficult to detect, and technicians need additional training in its use. Judges and attorneys alike need to develop a healthy skepticism towards evidence produced by digital technology.<sup>7</sup>

Courts and trial attorneys should address upfront the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings so that challenges to the evidence are not made for the first time at trial.<sup>8</sup> When the evidence is voluminous, it may be necessary to verify the evidence by sampling the data and, if errors are made, by stipulating or agreeing to the effect of the observed errors on the entire compilation. Statistical methods may also be used to determine the range and probability of error. (*Id.*) Computer evidence generated by a standard publicly available software may be more easily admitted than evidence generated by customer proprietary software. (*Id.*) Simply put, an attorney must make reasonable pretrial inquiries into the validity and source of digital information prior to attempting to use that information in court.<sup>9</sup>

In order to ensure ESI is actually admitted at trial requires the trial attorney to focus in pretrial proceedings to satisfy basic evidentiary concerns such as foundation and authenticity. This process is complicated by the fact that ESI comes in “multiple evidentiary flavors.”<sup>10</sup>

## II. INTRODUCTION TO ESI AUTHENTICITY ISSUES

Authenticating ESI poses many of the same issues as authenticating other evidence; however, introducing ESI may be more complicated because of the different format in which the record is maintained.<sup>11</sup> The degree of foundation required to authenticate ESI depends on the completeness and quality of the data input, the complexity of the computer processing, how routine the computer operation is, and the ability to test and verify results of the computer processing.<sup>12</sup>

Under both the Federal Rules and the Oklahoma Evidence Code, authenticity or identification as a condition precedent to admissibility is generally satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. The requirement ensures the evidence is trustworthy which can be especially important when a hearsay objection is raised.<sup>13</sup> Judge Weinstein notes that 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 § 901.02[3]. One court addressed the admissibility of e-mails by stating:

The 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, only that there is sufficient evidence that the *jury* ultimately might do so.<sup>14</sup>

(Emphasis in original.)<sup>15</sup> Thus, it is critical for the trial attorney to assimilate in advance of trial the necessary evidence to establish this basic fact and identify the witnesses who can provide the necessary testimony.

While this basic fact appears on its face easily satisfied, the reporters are littered with cases where counsel has failed to make even this minimal showing, resulting in what has been called a “self-inflicted injury.”<sup>16</sup> See *In re Vee Vinhnee, supra* (proponent failed properly to authenticate exhibits of electronically stored business records); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (proponent failed to authenticate exhibits taken from an organization’s website); *St. Luke’s Cataract & Laser Inst., P.A. v. Sanderson*, 2006 WL 1320242 at \*\*3-4 (M.D. Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Uncle Henry’s, Inc. v. Plaut Consulting, Inc.*; 240 F. Supp. 2d 63, 71-72 (D. Me. 2003), *aff’d* 399 F.3d 33 (1st Cir. 2005) (failure to authenticate e-mails); *Rambus, Inc. v. Infineon Tech. AG*, 348 F. Supp. 2d 698 (E.D. Va. 2004) (proponent failed to authenticate computer-generated business records); *Wady v. Provident Life & Accident Ins. Co. of America*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining an objection to affidavit of witness offered to authenticate exhibits that contained documents taken from defendant’s website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Ass’n, Inc. v. Wiley*, 1998 WL 1988826 at \*7 (S.D. Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results and, therefore, failed to authenticate them).

Courts often demand that the proponents of ESI pay more attention to foundational requirements than has been customary for introducing evidence not produced from electronic sources.<sup>17</sup> Judge Weinstein, in his treatise on evidence, explains that issues regarding the admissibility of electronic records is a fact-intensive issue. If the records are merely stored in a computer, they raise no computer-specific authentication issues. On the other hand, if the computer processes data rather than storing it, authentication issues may arise depending on the complexity and novelty of the computer processing. Because there are many stages in the development of computer data where error can be introduced which can adversely affect the accuracy and reliability of the input, greater scrutiny may be required. Inaccurate results occur often because of bad or incomplete data input but can also happen when defective software programs are used or stored data media becomes corrupted or damaged.<sup>18</sup> Thus, Judge Weinstein concludes the degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer proceedings. “Determining what degree of foundation is appropriate in any given case is in the judgment of the court. The required foundation will vary not only with the particular circumstances but also with the individual judge.” *Id.*

Fed. R. Evid. 901(b)(1)-(10) provides many examples of how authentication may be accomplished and should be consulted and used as ESI is being gathered in discovery. The ten (10) methods identified by Rule 901(b) are non-exclusive. See Committee Note to Fed. R. Evid. 901(b) (“The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law.”).<sup>19</sup>

At bottom, the requirement of authentication is an implicit function of applying Rule 402, which excludes from admission evidence that is not relevant.<sup>20</sup> To add probative value under Rule 401, evidence must bear some connection to the case. Without authenticating the evidence by showing that it is genuine and what it purports to be, a mandatory first step in determining whether the evidence is relevant has been overlooked. The Advisory Committee Notes to Rule 901 describe it as “inherent, logical necessity.” If the evidence is not what a proponent claims to be, it is irrelevant and inadmissible.<sup>21</sup>

### **III. USING CASE LAW UNDER FED. R. EVID. 901(b) TO GUIDE PRETRIAL DISCOVERY**

**A. Rule 901(b)(1) - *Testimony by a Witness with Personal Knowledge.*** In *United States v. Kassimu*, 2006 WL 1880335 (5th Cir. July 7, 2006), the Court held copies of a post office’s computer records could be authenticated by a custodian of the records, even though the witness neither personally entered the data nor had knowledge sufficient to testify about its accuracy. The court found the witness laid the proper foundation for introduction of the evidence because he was familiar with the procedure by which the records were generated. With respect to website printouts, one court found that a printout showing what a website looked like at various dates in the past was properly authenticated by an affidavit of the administrative director of the internet archive.<sup>22</sup> The director’s affidavit verified that copies were accurate reflections of the website on the particular dates on the internet archive’s records and described in detail the process used to allow visitors to search the archives.

One court, while noting that e-mails may be authenticated by a witness with knowledge that the exhibit is what it claimed to be, held that authentication may not be made by individuals who are not personally familiar with the e-mail<sup>23</sup>. Likewise, authentication of websites by testimony or affidavits of individuals who are not personally familiar with how the website is maintained are generally not permitted.<sup>24</sup> These cases illustrate that simply because you are able to locate and obtain ESI in discovery, in order to use it you must identify, depose and/or list the witnesses who can testify with the requisite personal knowledge that the ESI is what the proponent says it is.

**B. Rule 901(b)(3) - *Comparison by Trier of Fact or Expert Witness.*** Several courts have found that ESI could be authenticated by comparison to other ESI or evidence which had already been authenticated. For example, in *Safavian*, the court allowed e-mails, which were not clearly identifiable on their own, to be compared to other e-mails alleged to be from the same sender, which had been authenticated under Rule 901(b)(4).<sup>25</sup> The court stated the argument that the trustworthiness of these e-mails could not be demonstrated, particularly ones forwarded by others, went to the weight of the evidence and not authenticity.<sup>26</sup> The consideration of this rule should lead the lawyer to focus in pretrial proceedings on identifying ESI, such as e-mails, which will be easily admitted and then analyzing and strategizing how this evidence can be used to admit more difficult ESI into evidence.

**C. Rule 901(b)(4) - Evidence Containing Distinctive Characteristics.** Evidence of distinctive characteristics is a frequently used method of attempting to authenticate e-mails and other electronic documents. The type and scope of what must be shown in order to authenticate ESI under this Rule appears to be largely up to each individual judge; however, the courts have identified some common factors such as e-mail addresses and the use of names and nicknames throughout the correspondence.

In an Eleventh Circuit case, the court held that e-mails allegedly sent by the defendant were properly authenticated under Rule 901(b)(4).<sup>27</sup> The circumstantial evidence presented was the presence of defendant's known work e-mail address, the discussion of details the defendant would have been personally familiar with, use of the defendant's nickname, and a conversation with the recipient that was consistent with the e-mail conversation. *Id.* In *Safavian*, the district court allowed authentication of e-mails under Rule 901(b)(4) relying on almost identical circumstantial evidence.<sup>28</sup> In another case, the court allowed an instant message conversation to be authenticated under similar circumstantial evidence, including the presence of a known screen name, use of correct first name, and content the alleged participant was familiar with.<sup>29</sup>

Two other methods of authenticating ESI under 901(b)(4) are through "hash marks" and metadata. Hash marks are a unique numerical identifier which can be assigned to documents and groups of documents. Commonly used hash mark algorithms can reduce the chances of two documents having the same hash marks to less than one in a billion. Hashing can be used as the digital equivalent of the Bates stamp.<sup>30</sup> To date, it does not appear that many courts have directly addressed authentication by hash marking. For a detailed discussion of "hash marking,"<sup>31</sup>

Metadata refers to the data surrounding the creation and use of a document, such as file name, format, location, dates, and permissions. Courts have addressed metadata more in regards to discovery; however, it can provide useful information for authentication purposes. Nevertheless, since metadata is not a perfect source of information, it alone may not be enough to properly authenticate an electronic document.<sup>32</sup> Thus, pretrial discovery of metadata can be critical to authenticating important ESI.

Simply put, Rule 901(b)(4) places many tools in the pretrial arsenal to allow a trial attorney to use the ESI he or she gets. A trial attorney should have a very good understanding of the rule and its construction well in advance of trial to ensure the presentation of your case is seamless.

**D. Rule 901(b)(7) - Evidence That A Writing Authorized by Law Is From a Public Office Where Items of a Similar Nature Are Kept.** Courts have permitted authentication of electronic records by proof that the document was obtained from the legal custodian of those records. In *United States v. Meienberg*, *supra*, the Tenth Circuit held that print outs of approval numbers by the Colorado Bureau of Investigation for defendant's business were properly authenticated.<sup>33</sup> The court found authentication of electronic public records only required a showing of custody by the Bureau, and did not require a showing of accuracy as would be required by Rule 901(b)(9). *Id.* Thus, the burden of authenticating is substantially less under Rule 901 (b)(7), as opposed to 901(b)(9). There is a lot of valuable information relevant to a case publically available on governmental websites. Courts have shown a tendency to trust this

information making it easy to get into evidence. Always consider these sources in advance of trial and list them on your exhibit list with authenticating witnesses on your witness list.

**E. Rule 901(b)(9) - Evidence Describing a Process or System Used to Produce a Result and Showing that the Process or System Produces an Accurate Result.** This Rule was specifically designed to encompass computer generated evidence. Fed. R. Evid 901(b)(9) Advisory Committee Note. The Ninth Circuit Bankruptcy Appellate Panel applied a demanding eleven-step test for authenticating an electronic record under Rule 901(b)(9).<sup>34</sup> Under the test, developed by Professor Imwinkelried, a proponent of ESI must show: (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 good state of repair; (6) the witness had the computer read out certain data; (7) the witness used the proper procedure to obtain the readout; (8) the computer was in working order at the time the witness obtained the readout; (9) the witness recognized the exhibit as the readout; (10) the witness explains he or she recognizes the readout; (11) if the readout contains any strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact. *Id.* at 446. The *Vinhnee* court found that the foundational witness had not met all steps of this test because he had no knowledge about the computers processes and could not assure the accuracy of the results. *Id.* at 448. At this point, it does not appear that any other cases have adopted this test; however, it is a standard that attorneys should be prepared to meet. Thus, a good pretrial practice is to use this test as a guide to ensure that you have discovered and are prepared to introduce the evidence and witnesses necessary to establish each of these requirements.

#### **IV. PRETRIAL PRACTICES RELATED TO SPECIFIC TYPES OF ESI**

**A. E-mails.** Most of us have become so familiar with e-mails that we now consider them like business letters, to be admitted into evidence just as easily. However, e-mails may be more prone to problems of authenticity (and hearsay) than one might consider at first blush. E-mails are often written casually, and may be fraught with jokes, informality, poor grammar and little care given to context. Signatures and names may be omitted. Thus, authenticating e-mails presents issues not faced with traditional letters containing letterhead, paragraph structures, signatures, etc. Moreover, e-mail messages are more susceptible to after-the-fact alteration.

For example, most e-mail systems allow one to edit to an e-mail message being forwarded. Generally, such alteration is not obvious to the recipient. E-mail chains present hearsay within hearsay problems. Such chains attach to an e-mail every e-mail that came before it in a discussion. What is one to do to try to get an e-mail into evidence when it is necessary to get all the other prior e-mails to be separately authenticated and found admissible?

Authentication is necessary not only at trial but also at the summary judgment stage. For example, we should always be prepared to submit evidence in the form of affidavits to support the authenticity of any e-mail that one intends to introduce. Courts have excluded e-mails at the time of the dispositive motion not because the e-mails were clearly inauthentic but because evidence was not submitted to support their authenticity in the face of a challenge.<sup>35</sup>

Because of the spontaneity and informality of e-mails, courts seem to think people are “more themselves” for better or worse, than other deliberative forms of written communication.<sup>36</sup> Thus, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved.<sup>37</sup> E-mails are often authenticated under Rules 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), 901(b)(4) (distinctive characteristics, including circumstantial evidence), 902(7) (trade inscriptions), and 902(11) (certified copies of business record).<sup>38</sup>

Because it can be difficult to prove authorship of an e-mail, i.e., who actually wrote the message, other means to authenticate it may be necessary. There are several technical means by which such evidence can be traced to its origins. This can be done through internet service providers, cellular phone companies, password or access codes, etc. However, identifying the actual person that wrote the message may not be as easy since all one has to do to gain access to that person’s computer, cellphone, etc., is to obtain the password or pass code. Indeed, access to the other person’s actual device is not even necessary as the person can log in from their own computer

The point is obvious. Rule 901(b)(4) permits authentication by “distinctive characteristics.” This authentication method is authentication by “circumstantial evidence,” Weinstein at § 901.03[8], and has been successfully used to authenticate e-mails. *See Siddiqui*, 235 F.3d 1318; *Safavian, supra* (where e-mails frequently contained the name of the sender and recipient in the bodies of the e-mails, in the signature blocks of the e-mail, in the “to” and “from” headers, and by the signature of the sender and often referred to various professional and personal matters known to the defendant).

The *Lorraine* court suggested any electronic document can be authenticated under 901(b)(4) using metadata. Metadata is “data about data.” *See Netword LLC v. Centraal Corp.*, 242 F.3d 1347, 1354 (Fed. Cir. 2001); *see also* Fed. R. Civ. P. 26(p) Advisory Committee Note (describing metadata); THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES AND COMMENTARY FOR MANAGING INFORMATION AND RECORDS IN THE ELECTRONIC AGE. “Because metadata shows the date, time, and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all ESI that can be used to authenticate it under Rule 901(b)(4).” *Lorraine*, 241 F.R.D. at 547-48. Again, pretrial discovery of metadata can be crucial to ensure important ESI gets into evidence.

Because electronic mail can contain critical evidence, it is imperative that one consider these authenticity issues at the start of the case and prepare your discovery plan to ensure that such evidence is actually admitted. Finally, it should be noted that access to private e-mail and voice mail is regulated by Title 2 of the TCPA commonly known as the Stored Communications Act, 18 U.S.C. §§ 2701-2711. There is no exclusionary rule under that Act so that voice mail or e-mail, even when accessed through a violation of the Act, is still admissible.

**B. Instant Messages and Text Messages.** Like e-mails, instant messages and text messages can be authenticated by evidence sufficient to support a finding that the matter in question is what its proponent claims. It can also be admitted based on distinctive characteristics such as appearance, content, substance, internal patterns and other distinctive characteristics taken in conjunction with the circumstances.<sup>39</sup>

Instant messages and text messages also present different problems than other types of ESI, such as e-mails or telephone conversations. With e-mails, a party exchanges messages with a person who is likely known to him personally or whose identity is likely known to the owner or operator of the e-mail server, such as a school or business. In a telephone conversation, a party may be identified by his voice or locution, and there is a presumption that if a party picks up the phone and identifies himself as the person listed at that number in the phone book, he is indeed that person.<sup>40</sup>

Those of us who have teenagers know of the prevalent use of instant messages and text messages. The top 5 instant messaging services have nearly a 170 million active users among them.<sup>41</sup> Over 50% of workers use instant messaging software and U.S. internet users between 12 and 17 years of age prefer instant messaging to e-mail. *Id.* Many of our jurors will have used and be conversant with “IM.” Thus, use of this type of evidence will become more and more frequent. The issues surrounding instant messaging are complex. For those who have an especially knotty instant messaging evidentiary issue, I refer you to Grossman’s Law Review article cited above which contains an excellent 26-page discussion surrounding these issues.

**C. Websites.** Internet websites have often been viewed with much skepticism.<sup>42</sup> Other courts have taken a more permissive approach.<sup>43</sup> Most courts hold that websites are not self-authenticated under Rule 902.<sup>44</sup>

The issues that have concerned the courts regarding websites include the possibility that third persons, other than the sponsor of the website, were responsible for the content of the postings, such as a hacker (without the owner’s consent) or a third party (with the owner’s consent). Because websites have become increasingly interactive, additional issues arise. People can shop and make purchases on websites, participate in surveys, sign contracts, post comments, provide videos, music, pictures – all on other people’s websites. When this conduct becomes relevant to a dispute, it becomes evidence.

Rule 901(b)(1) (testimony from a witness with knowledge) is often used to authenticate websites, but the courts differ on how much knowledge is necessary. For example, the Seventh Circuit excluded evidence of website postings because the proponent failed to show that the sponsoring organization actually posted the statements, as opposed to a third party.<sup>45</sup> In that case, the court required such proof to insure that the information was not “slipped onto the group’s web sites by the [defendant] herself, who was a skilled computer user.” *Id.* In *St. Luke’s*, the court excluded website postings because the affidavit used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge.<sup>46</sup>

Three questions must be answered explicitly or implicitly with websites: (1) what was actually on the website; (2) does the exhibit or testimony accurately reflect it; (3) if so, is it attributable to the owner of the site?<sup>47</sup> Judge Weinstein goes on to identify several factors courts should consider in admitting evidence of internet postings.<sup>48</sup>

A witness may be able to authenticate website data by showing (1) the witness typed in URL (the www. address), (2) logged into the site, (3) reviewed what was there, and (4) testified that the printout or other exhibit fairly and accurately reflects it. Web pages also involve HTML

(hyper text markup language) codes. That is a document used on the internet that provides that text and extra information about the text, i.e., its structure and presentation. Web pages are built with HTML tags or codes imbedded in the text and it defines the page layout, fonts and graphic evidence as well as hyper text's links to other documents on the web.<sup>49</sup>

**D. Chat Rooms.** Many of the same foundational issues present in addressing e-mails and text messages are present in chat room content. Nevertheless, the fact that chat room messages are posted by third parties often using "screen names," means that it cannot be assumed that the content found in chat room is posted with the knowledge or authority of the website host. *See* Saltzburg at § 901.02[12]. Thus the transcript is almost always authenticated under Rule 901(b)(4) using circumstantial evidence.<sup>50</sup> Saltzburg suggests the following foundational requirements must be met to authenticate chat room evidence:

- (1) Evidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
- (2) [e]vidence that, when a meeting with the person using the screen name was arranged, the individual ... showed up;
- (3) [e]vidence that the person using the screen name identified [himself] as the [person in the chat room conversation];
- (4) [e]vidence that the individual had in [his] possession information given to the person using the screen name;
- (5) [and] [e]vidence from the hard drive of the individual's computer [showing use of the same screen name].

Saltzburg, § 901.02[12]. Discovery to uncover evidence to meet these basic foundational steps will allow the trial attorney to meet most chat room authenticity objections.<sup>51</sup>

**E. Voice Mail, Tape-Recorded Conversations, Digital Video and Audio Recordings.** Generally, the foundation for this type of evidence can be shown by a witness who is familiar with the objects seen or sound that is depicted in the recording, then explains the basis for his or her familiarity and testifies that the recording is a fair, accurate, true or good depiction of what it purports to be at the relevant time. Other factors may include showing that the recording device was capable of making the recording and was operational; showing that the operator of the device was competent; establishing the authenticity or correctness of the recording; showing that changes, additions or deletions had not been made; showing the manner of the preservation of the recording; identifying speakers (if relevant), and other similar factors.

Because such recordings are now "digitized," i.e., made from images and can be loaded on the computer, they present unique authentication problems because they are a form of electronically-produced evidence that may be manipulated and altered. Digital recordings and photos may be "enhanced," such as removing, inserting or highlighting an aspect that the technician wants to change.<sup>52</sup> Professor Imwinkelried identifies numerous problems with digital photographs which also applies to all other types of digital recordings.

Original digital recordings may be authenticated the same way as other such evidence, i.e., by a witness with personal knowledge of the scene depicted who can testify that the recording or photo fairly and accurately depicts it. If the recording or photograph has been digitally converted, authentication requires an explanation of the process by which it was

converted to a digital format. This would seem to require a witness with personal knowledge that the conversion process produces accurate and reliable images and perhaps expert testimony. For digitally enhanced images, it is likely that an expert will be required. Professor Imwinkelried's article on digital photos is an excellent resource on these issues. The point is again basic. Careful pretrial planning regarding your ESI is essential to a litigant's success.

**F. Electronically-Stored Records and Data.** Judge Weinstein observes that there are a limitless variety of records stored or generated by computers in the modern age. “[M]any kinds of computer records and computer-generated information are introduced as real evidence or used as litigation aids at trials. They range from computer printouts of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements.”<sup>53</sup>

With respect to electronically-stored records, the attorney should locate and prepare a witness who can testify (1) regarding their familiarity with the computer-stored records and explain the basis for his or her familiarity; (2) that the witness recognizes the paper records as being a printout of the computer-stored records; and (3) that the paper records accurately reflect the computer-stored records. “In general, electronic documents are records that are merely stored in a computer and raise no computer specific authentication issues.” Weinstein at § 900.06[3]. Nevertheless, many sources suggest that more care is required to authenticate these electronic records than traditional “hard copy” records.<sup>54</sup>

**G. Computer-Generated Records.** Computer-generated records differ from computer-stored records in many ways. For example, graphs, tables, animations, slide shows and spreadsheets are all computer-generated records. Thus, issues arise such as whether the computer that generated the records was functioning properly.<sup>55</sup> Establishing the reliability of a system or process does not necessarily require the testimony of an expert.<sup>56</sup> Moreover, the witness who testifies concerning the authenticity of computer-generated records does not need to have programmed the computer himself or even understand the maintenance and technical operation of the computer.<sup>57</sup> Nevertheless, it should be remembered that the computer can only process the data given to it, so if that data is in error and the error goes undetected, the output would be in error. Likewise, the computer can only process the data as it is instructed to process, so if that data is incomplete or inaccurate, the output would be error. If there is a deficiency in the manner in which the computer is told to process the data, the output would likewise be in error. Good results are obtained when programs are carefully prepared by trained professionals who understand how programs work and use them accordingly.<sup>58</sup>

Among the factors courts may apply in determining whether a proper foundation for admission of computer-generated evidence has been laid include whether the computer was standard and in good working order, whether the operators of the equipment were qualified, whether proper procedures were followed, whether reliable software was used, whether the program operated properly, and the exhibit derived from the computer.<sup>59</sup> In that case, the court stressed that “these factors represent an approach to the admissibility of computer generated evidence and are not a mechanical, clearly defined test with a finite list of factors to consider.”). *Id.* Discovery relating to each of these factors is present in the pretrial stage to permit effective use of your computer-generated information.

**H. Computer Animations and Computer Simulations.** Computer animations and computer simulations also raise unique evidentiary issues.<sup>60</sup> Because of the persuasive power of demonstrative evidence, such as animations and simulations, courts are obligated to make a thorough foundational inquiry into its reliability before admitting it, giving the potential that it may mislead, confuse, divert or otherwise prejudice purposes of a trial if not reliable.<sup>61</sup> The court in *Sayles* explained the difference between computer animations and computer simulations as follows:

Computer generated evidence is an increasingly common form of demonstrative evidence. If the purpose of the computer evidence is to illustrate and explain a witness' testimony, courts usually refer to the evidence as an animation. In contrast, a simulation is based on scientific or physical principles and data entered into a computer, which is programmed to analyze the data and draw a conclusion from it, and courts generally require proof to show the validity of the science before the simulation evidence is admitted.<sup>62</sup>

The *Lorraine* court reviewed the cases and observed that courts have generally allowed the admission of computer animations if authenticated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help illustrate the testimony given in the case.<sup>63</sup> In *Friend v. Time Mfg. Co.*, 2006 WL 2135807 at \*7 (D. Ariz. July 28, 2006), the court held that, at a minimum, with respect to animations, the proponent must show the computer simulation fairly and accurately depicts what it represents, whether through the computer expert who prepared it or some other witness who is qualified to so testify. The opposing party must then be afforded an opportunity for cross-examination.

On the other hand, computer simulations are treated as a form of scientific evidence offered for a substantive, rather than demonstrative, purpose.<sup>64</sup> Courts often treat such simulations like other scientific tests and condition admissibility upon showings that (1) the computer is functioning properly; (2) the input and underlying equations are sufficiently complete and accurate (and disclosed to the opposing party so that they may challenge them); and (3) the program is generally accepted by the appropriate community of scientists.<sup>65</sup>

The *State v. Swinton* case, *supra*, adopted the *Commercial Union* case but added that the key to authenticating computer simulations is to determine their reliability. The court noted that the problems that could arise with such evidence include (1) the underlying information itself could be unreliable; (2) the entry of the information in the computer could be erroneous; (3) the computer hardware could be unreliable; (4) the computer software programs could be unreliable; (5) the execution of the instructions which transforms the information in some way – for example, by calculating numbers, sorting names or storing information or retrieving it later – could be unreliable; (6) the output of the computer, such as the printout transcript or graphics, could be flawed; (7) the security system used to control access to the computer could be compromised; and (8) the user of the system could make errors.<sup>66</sup>

## V. CONCLUSION

Aside from good facts, trials are often won by hard work, advance planning, a thorough understanding of the law applicable to your case and creative presentation. The understanding and use of the law of authenticity as it relates to ESI at the start of the case will go a long way to ensuring the ESI you discover will be admitted to help win the case.

- 
1. See, however, proposed Fed. R. Evid. 502 relating to privilege issues surrounding the inadvertent production of electronic evidence.
  2. For sake of uniformity, the Federal Rules of Evidence will be most often referred to in this paper, although the same analysis will often apply equally to the companion rules, such as the Oklahoma Evidence Code.
  3. See *Novartis Corp. v. Ben Venue Labs., Inc.*, 271 F.3d 1043, 1054 (Fed. Cir. 2001) (holding that the foundation and methodology of computer programs must be disclosed to satisfy evidentiary requirements and allow meaningful cross-examination).
  4. See *Manual for Complex Litigation* (Fourth), § 11.446.
  5. See *In re Vee Vinhnee*, 336 B.R. 437, 444-45 (B.A.P. 9th Cir. 2005) (adopting Professor Imwinkelried's eleven-step process for authenticating computer records, stating "[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.").
  6. *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999) (referring to information taken from the internet as "voodoo"). See also *Terbush v. United States*, 2005 WL 3325954 at \*5 (E.D. Cal. Dec. 7, 2005) ("Information on internet sites presents special problems of authentication.").
  7. Imwinkelried, *Digitized Evidence* (NAT'L L. J. Mar. 7, 2005).
  8. *Manual for Complex Litigation* (Fourth), § 11.446.
  9. See *Jimenez v. Madison Area Tech. College*, 321 F.3d 652, 658 (7th Cir. 2003) (imposing Rule 11 sanctions on plaintiff and plaintiff's attorney where court found that e-mails were "obviously fraudulent").
  10. See *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534, 538 (D. Md. 2007) (perhaps the most expansive and detailed opinion addressing admissibility of electronically stored information and an excellent resource for this paper) (hereinafter referred to as "*Lorraine*").
  11. *In re Vee Vinhnee*, 336 B.R. 437 (B.A.P. 9th Cir. 2005).
  12. *Lorraine*, 241 F.R.D. at 544.
  13. See Weinstein at § 901.02[2].
  14. *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006).
  15. See also *United States v. Meienberg*, 263 F.3d 1177, 1180 (10th Cir. 2001) (computer records printouts); *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (chat room conversations); *United States v. Reilly*, 33 F.3d 1396, 1404 (3d Cir. 1994) (radio telegrams); *Telewizja Polska USA, Inc. v. EchoStar Satellite Corp.*, 2004 WL 2367740 at \*16 (N.D. Ill. Oct. 15, 2004) (website content).
  16. *Lorraine*, 241 F.R.D. at 542 (dismissing cross motions for summary judgment for failure to authenticate).
  17. *Lorraine*, 241 F.R.D. at 543.
  18. Weinstein at § 900.06[3].
  19. See also *United States v. Simpson*, 152 F.3d 1241, 1249 (10th Cir. 1998) (evaluating methods of authenticating a printout of the text of a chat room discussion between the defendant and an undercover detective in a child pornography case stating examples of authentication in the rule are "merely illustrative" and "are not intended as exclusive enumeration of allowable methods of authentication.").
  20. See Weinstein at § 900.06[1][a].
  21. See *United States v. Meienberg*, 263 F.3d 1177, 1181(10th Cir. 2001) ("The rationale for the authentication requirement is that the evidence is viewed as irrelevant unless the proponent of the evidence can show that the evidence is what its proponent claims.").
  22. *Telewizja Polska USA, Inc. v. EchoStar Satellite Corp.*, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004).

- 
23. *Safavian*, 435 F. Supp. 2d at 40.
  24. *See St. Luke's Cataract & Laser Inst., P.A. v. Sanderson*, 2006 WL 1320242 (M.D. Fla. May 12, 2006); *Wady v. Provident Life & Accident Ins. Co. of America*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002).
  25. *Safavian*, 435 F. Supp. 2d at 40.
  26. *Id.* at 40-41.
  27. *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000).
  28. 435 F. Supp. 2d at 39-41.
  29. *In re F.P.*, 878 A.2d 91, 94 (Pa. Super. Ct. 2005) (interpreting state rule similar to the federal rule 901(b)(4)); *see also United States v. Jackson*, 208 F.3d 633 (7th Cir. 2000) (finding that web postings were not properly authenticated under Rule 901(b)(4)); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153 (C.D. Cal. 2002) (finding website postings were properly authenticated using circumstantial evidence such as correct dates and web address).
  30. *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. at 546-47 (*quoting* Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges* (2007), at 24).
  31. *See Hash, The New Bates Stamp*, 12 J. TECH. L. & POL'Y 1.
  32. *See Fenell v. First Step Designs, Ltd.*, 83 F.3d 526, 530 (1st Cir. 1996) (discussing how saving files in different locations and not changing the text may cause change in metadata markers).
  33. *Meienberg*, 263 F.3d at 1180-81.
  34. *In re Vee Vinhnee*, 336 B.R. at 446-47.
  35. *See Bouriez v. Carnegie Mellon Univ.*, 359 F.3d 292 (3d Cir. 2004).
  36. *See Lorraine*, 241 F.R.D. at 554.
  
  37. *See Safavian*, 435 F. Supp. 2d 36.
  38. *Lorraine*, 241 F.R.D. at 554.
  39. *See* Fed. R. Evid. 901(b)(4).
  40. *See* Fed. R. Evid. 901(b)(6).
  41. *See Grossman, No, Don't IM Me - Instant Messaging Authentication of the Best Evidence Rule*, 13 GEO. MASON L. REV. 1309 at fn. 11.
  42. *See St. Clair*, 76 F. Supp. 2d 773 (S.D. Tex. 1999) (holding that there is a presumption that information discovered on the internet is inherently untrustworthy and "voodoo" information as websites are not monitored for accuracy and nothing contained on the website is under oath or even subject to independent verification absent underlying documentation).
  43. *See Perfect 10*, 213 F. Supp. 2d at 1153-54 (finding that internet website postings were authenticated because of circumstantial indicia of authenticity and a failure of the defendant to deny their authenticity).
  44. *See Sun Protection Factory, Inc. v. Tender Corp.*, 2005 WL 2484710 (M.D. Fla. Oct. 7, 2005); *Ashworth v. Round Lake Beach Police Dep't.*, 2005 WL 1785314 (N.D. Ill. Jul. 21, 2005).
  45. *Jackson*, 208 F.3d at 637-38.
  46. *See also Novak v. Tucows, Inc.*, 2007 WL 922306 at \*5 (E.D.N.Y. Mar. 26, 2007) (website printouts are not authenticated because plaintiff offered no testimony or sworn statements by employee of company hosting the sites); *Illusions-Dallas Private Club, Inc. v. Steen*, 2005 WL 1639211 at \*10 (N.D. Tex. Jul. 13, 2005), *rev'd on other grounds*, 482 F.3d 299 (5th Cir. 2007) (attorney affidavit insufficient to authenticate website because no personal knowledge that studies were what they claimed to be); *Costa v. Keppel Singmarine Dockyard PTE, Ltd.*, 2003 WL 24242419 at \*7 (C.D. Cal. Apr. 24, 2003) (same result on affidavit by downloading witness).
  47. Weinstein at § 901.02[21].
  48. Weinstein at § 901.02[22].
  49. *See ACTONet, Ltd. v. Allou Health & Beauty Care*, 219 F.3d 836 (8th Cir. 2000).
  50. *See United States v. Tank*, 200 F.3d 627 (9th Cir. 2000); *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998).
  51. *See also United States v. Simpson*, 152 F.3d at 1249; *United States v. Tank*, 200 F.3d at 629-31.
  52. *See* Edward J. Imwinkelried, *Can This Photo Be Trusted at Trial* (October 2005) at 48.
  53. Weinstein at § 900.06[3].
  54. *See Manual for Complex Litigation* at § 11.447; Imwinkelried, *Evidentiary Foundations* at § 4.03[2] ("[F]ollowing the recommendations of the Federal Judicial Center's *Manual for Complex Litigation*, some courts now require more extensive foundation [for computer-stored records]. These courts require the proponent to

---

authenticate a computer record by proving the reliability of the particular computer used, the dependability of the business's input procedures for the computer, the use of proper procedures to obtain the document offered in court, and the witness's recognition of that document as the readout from the computer."').

55. See 2 *McCormick on Evidence*, § 294 at 286 (John William Strong, et al., 4th ed. 1992); Saltzburg at p. 370.

56. See *United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001).

57. See *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991).

58. See Roberts, *A Practitioner's Primer on Computer-Generated Evidence*, 41 U. CHI. L. REV. 254, 263-64 (1974).

59. See *State v. Swinton*, 847 A.2d 921, 942-43 (Conn. 2004).

60. See Imwinkelried, *Evidentiary Foundations* at § 4.09[4][a].

61. See, e.g., *Taylor v. United States*, 759 A.2d 604, 608 (D.C. 2000); Hanon, *Computer Generated Evidence: Testing the Envelope*, 63 DEF. COUNS. J. 353, 361 (1996).

62. *State v. Sayles*, 662 N.W.2d 1, 9 (Iowa 2003).

63. 241 F.R.D. at 559-60 (citing cases).

64. Weinstein at § 900.03[1]; Imwinkelried, *Evidentiary Foundations* at § 4.09[5][a], [c].

65. See *Commercial Union Ins. Co. v. Boston Edison Co.*, 591 N.E.2d 165, 168 (Mass. 1992).

66. 847 A.2d 921, 942-43.