

ADMITTING EMAIL AND OTHER ELECTRONIC EVIDENCE

Inns of Court Presentation
March 13, 2012
Judge Farley's Group

I. WHERE TO START?¹

1. Is the ESI **relevant**? FRE 401 sets forth the test: does the ESI 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, is it **authentic**? FRE 901(a) requires that the proponent show the ESI is what it purports to be.
3. Is the ESI **hearsay**? Is it offered for its substantive truth? Is it hearsay as defined by FRE 801? Is it covered by an applicable exception under FREs 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? Is there admissible secondary evidence to prove the content of the ESI under FREs 1001-1008?
5. Is the **probative value of the** ESI **substantially outweighed** by the danger of unfair prejudice or is it otherwise inadmissible under FRE 403?

II. RELEVANCE: THE EASY FIRST STEP.

Although evidence that is not relevant is never admissible, Fed R. Evid. 402, establishing that ESI has some relevance is fairly easy. As with any evidence, relevance depends strictly on the issue and purpose for which that evidence is offered. Evidence inadmissible for one purpose, may be admissible, for another.

III. AUTHENTICATION: IT IS WHAT IT IS ISN'T IT?

Authenticity requires that the proponent offer admissible evidence from which the jury can reasonably conclude that the ESI is what it is claimed to be. Under FRE 104(b), such foundation must, itself, be admissible evidence. The following provisions most frequently apply to ESI:

FRE 901 (b)(1) KSA § 60-465	Authentication by: "[t]estimony that a matter is what it is claimed to be." The requirement is generally liberally interpreted. Although Rule 901(b)(1) is met by the testimony of a witness that actually drafted the exhibit, it is not required that the authenticating witness have personal knowledge of the making of a particular exhibit if he or she has personal knowledge of how that type of exhibit is routinely made. It is necessary that the authenticating witness provide factual specificity about the process by which the electronically stored information is, created, acquired, maintained, and
--------------------------------	---

¹ The Honorable Judge Grimm, Chief United States Magistrate Judge for the District of Maryland outlined an excellent evidentiary analysis in *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534 (D. MD. 2007). The structure of this outline is based on this opinion.

preserved without alteration or change, or the process by which it is produced. You should avoid the boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8).

FRE 901(b)(3)
KSA § 60-465

This rule allows authentication or identification by comparison by the trier of fact or by expert witnesses with specimens which have been authenticated. The specimen from which comparison is made must itself first be authenticated. The rule was originally utilized with handwriting and signatures. You can use this rule for the admission of e-mail.

FRE 901(b)(4)
KSA § 60-467

Authenticated or identified by "[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." This rule is one of the most frequently used to authenticate e-mail and other electronic records. Admissible evidence relating dates, screen names, e-mail addresses and identities, nicknames, web addresses and, conversational references to the content may be sufficient authentication under this rule.

Another way to insure authentication requires advance preparation. Judge Grimm indicates the hash values or marks are unique numerical identifiers that can be inserted into original documents at creation. The presence of the same hash value when offered into evidence establishes that the document is the same and unchanged, as even the slightest alteration would also alter the hash value. The hash marks can also be used as a form of electronic document numbering. Similar to an electronic bates number, Hash values/marks are particularly valuable for a proponent in introducing its own ESI into evidence. An attorney may also consider the use of metadata. Metadata, unlike hash marks/values, is automatically created by computer programs and does not require the forethought of hash values. Metadata is not a fool proof identifier and can be altered, intentionally or otherwise. An attorney should be careful of this. Despite its lack of conclusiveness, however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics.

FRE 901 (b)(7)
KSA § 60-469

Public records are regularly authenticated by proof of custody, without more. Rule 901(b)(7) extends the principle to include data stored in computers and similar methods, of which increasing use in the public records area - may be expected. Records which may be authenticated as public records include tax returns, weather bureau records, military records, social security records, INS records, VA records, official records from federal, state and local agencies, judicial records, correctional records, law enforcement records, and data compilations, which may include computer stored records. This list is not complete.

FRE 901 (b)(9)
KSA § 60-469

Authentication by "[e]vidence describing a process or system used to produce a result and showing that the processor system produces an accurate, result." This rule recognizes one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. Many courts are becoming increasingly demanding as to foundations in this area. The foundation required by the court in *In Re Vee Vinhnee*, 336 BR 437, 446 (B.A.P. 9' 2005) should be considered as an excellent model.

FRE 902

In addition to the non-exclusive methods of authentication identified in Rule 901(b), Rule 902 identifies twelve methods by which documents, including electronic ones, may be authenticated without extrinsic evidence. This is commonly referred to as "self-authentication."

Here are some common sense approaches to authentication:

E-mail

There are numerous ways to authenticate, e-mail, under both Rules 901 and 902. In all likelihood, e-mails bear the sender's e-mail address and often the entire chain of messages created by utilizing the reply function, providing a wealth of information beyond the simple e-mail text, much of which is useful for authenticating those e-mails. The most frequent ways to authenticate e-mail evidence are 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).

Website pages/
Data

Authentication of website evidence should address three questions: (1) what was actually on the website? (2) does the exhibit accurately reflect that content? (3) if so, can it be attributed to the owner of the site? 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), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications).

IM/Chat

Many of the same foundational issues found encountered when authenticating-website evidence apply to text messages and internet chat room content. One problem with chat room messages is they are often posted by third parties, often using "screen names." A lawyer cannot assume that the content found in chat rooms was posted with the knowledge or authority of the website host.

The rules most likely to be used to authenticate chat room and text messages, alone or in combination, appear to be 901(b)(1) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics).

Computer Stored/
Generated Files

Computers store an unlimited variety of information, in myriad forms, each form raising different authentication issues. “The least complex admissibility issues are associated with electronically stored records. ‘In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues.’ ... That said, although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional ‘hard copy’ record.” 241 F.R.D. 534, 557 Authentication should focus less 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.” *Id. at 558.*

It appears that the requirements for authentication of computerized records are changing. A prepared lawyer will know in advance the requirements to be imposed in their court.

Computer
Generated
Evidence

Computer generated evidence includes both animations and simulations. Classification as a simulation or animation will determine the type of foundation required. “If the purpose of the computer evidence is to illustrate and explain a witness’s 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 that validity of the science before the simulation evidence is admitted. *Id. at 559.* Animations are generally admitted on the authentication of the witness that it fairly and accurately portrays the facts and will help illustrate his/her testimony. Such animations are generally demonstrative, rather than substantive evidence. Simulations, however, are treated differently and offered as substantive evidence. “Computer simulations are treated as a form of scientific evidence, offered for a substantive, rather than demonstrative purpose.” *Id. at 560.*

Digital Photos

Due to their susceptibility to alteration, digital photographs present issues unknown with traditional photographs printed from film. Digital photographs should be considered as three distinct types, each with separate authentication issues: original digital images, digitally *converted* images, and digitally *enhanced* images.

“An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it. If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under Rule 201. For digitally converted images, authentication requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with

personal knowledge that the conversion process produces accurate and reliable images, Rules 901(b)(1) and 901(b)(9), the later rule implicating expert testimony under Rule 702. Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion.” *Id. at 561.*

Digitally enhanced images must be authenticated differently and treated as scientific evidence. “Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a means to authenticate digitally enhanced photographs under Rule 901(b)(9): (1) The witness is an expert in digital photography; (2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the process by which the computer manipulates them; (3) the witness testifies that the processes used are valid; (4) the witness testifies that there has been ‘adequate research into the specific application of image enhancement technology involved in the case’; (5) the witness testifies that the software used was developed from the research; (6) the witness received a film photograph; (7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer; (8) the witness can identify the trial exhibit as the product of the enhancement process he or she performed” *Id. at 562.*

IV. HEARSAY.

Hearsay issues are pervasive when electronically stored and generated evidence is introduced.” Before the proponent can relax, he/she must consider each of the following:

1. Is the evidence a statement under FRE 801(a)?
2. If so, was it made by a “declarant” under FRE 801(b)?
3. If so, is it being offered to prove the truth of its contents, as provided by Rule 801(c)?
4. Is it excluded from the reach of the hearsay by Rule 801(1)?
5. If its hearsay, is it exempted and admissible under Rules 803, 804 or 807?

FRE 801(a) & (b). Is the evidence a statement? The committee notes to FRE 801(a) address KSA § 60-459(a),(b) the issue as follows: “The effect of the definition of ‘statement’ is to exclude from the operation of the hearsay rule all evidence of conduct, verbal or nonverbal, not intended as an assertion. The key to the definition is that nothing is an assertion unless intended to be one.” *Id. at 563.* Also intertwined is whether the statement (if there is one) is made by a declarant.

Where a human speaker is not involved, neither is hearsay. When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no "person" involved in the creation of the record, and no "assertion" being made. For that reason, the record is not a statement and cannot be hearsay. *Id. at 564.*

FRE 801(c) Unless the statement is offered to prove the truth of the matter asserted, i.e., for its substantive truth, it is not hearsay. FRE 801(c). There are numerous circumstances where assertive statements are not hearsay because they are not offered to prove the truth of the assertions. Those circumstances include "(1) statements offered to prove a claim that the statement was false or misleading, as in a fraud or misrepresentation case; (2) statements offered to prove that because they were made, listeners had notice or knowledge of the information related in the statements, or to show the effect on the listener of the statement; (3) statements offered to prove an association between two or more persons; (4) statements offered as circumstantial evidence of the declarant's state of mind, or motive; (5) statements that have relevance simply because they were made, regardless of their literal truth or falsity--the so called 'verbal acts or parts of acts,' also referred to as 'legally operative facts'; and (6) statements that are questions or imperative commands, such as 'what time is it' or 'close the door.'" *Id. at 565-66.*

The same rules apply to electronic evidence; unless the evidence is offered to prove its own substantive truth, it is not hearsay.

FRE 801(d) The question of whether the evidence, otherwise hearsay, is, excluded by
KSA § 60-460(g) FRE 801(d)(1) or (2) also arises in considering ESI. Of primary concern, are admissions by a party under 801(d)(2).

Is the hearsay evidence exempted and admissible under Rules 803, 804 or 807? Between these rules there are 28 specific exemptions, plus one overarching "catch-all" provision. The 23 expectations of Rule 803 have been conveniently categorized by Judge Grimm:

Category 1 includes exceptions dealing with **perceptions, observations, state of mind, intent and sensation** (803(1) (present sense impressions); 803(2) (excited utterances); 803(3) (then existing state of mind, condition or sensation); 803(4) (statements in furtherance of medical diagnosis and treatment). **Category 2** includes **documents, records, and other writings** (803(5) (past recollection recorded); 803(6) & (7) (business records); 803(8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12) (certificates of baptism, marriage and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) (ancient documents); 803(18) (learned treatises); 803(22) (judgments of conviction in a

criminal case); and 803(23) (judgments in certain kinds of civil cases). **Category 3** includes statements dealing with **reputation** (803(19) (reputation regarding personal or family history); 803(20) (reputation regarding custom, use and practice associated with land, and historically significant facts); and 803(21) (reputation regarding character within the community and among associates). 241 F.R.D. at 568.

ESI may fit within the first category given the ubiquity of communications in electronic media (e-mail, text messages, chat rooms, internet postings on servers like "myspace" or "youtube" or on blogs, voice mail, etc.), it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium. It would unnecessarily prolong an already lengthy opinion to analyze all of the implications of the hearsay exceptions in Rule 803 as they relate to ESI. *Id.* at 568-69.

The business records exception found in Rule 803(6) is often analyzed in conjunction with Rule 902(11) in admitting ESI consisting of electronically stored records. The well known foundation is "(1) The document must have been prepared in the normal course of business; (2) it must have been made at or near the time of the events it records; (3) it must be based on the personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant; and (4) to have been made in the normal course of business means that the document was made in the regular course of a regularly conducted business activity, for which, it was the regular practice of the business to maintain a memorandum." *Id.* at 571.

V. ORIGINAL WRITING.

The advisory committee comments to Rule 1001 make clear that the original writings rule applies to electronic data. Rule 1002 requires that, to prove the contents of the item, the original of writings, recordings and photographs must be introduced, except as otherwise provided in the rules or other laws. The potentially thorny problems posed by this provision are largely avoided by Rule 1003, which makes duplicates freely admissible absent genuine issues of authenticity or, unfairness in admitting something less than an original.

Judge Grimm writes that under Rule 1001(3), "the 'original' of information stored in a computer is the readable display of the information on the computer screen, the hard drive or other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data." *Id.* at 577.

Rule 1004 defines situations when secondary evidence is admissible when the original is lost or destroyed. Rule 1004(1) addresses situations where the original is lost or unavailable and has particular application to electronic data.

Rule 1006 allows introduction of summaries in lieu of the contents of voluminous writings.

Kansas has similar rules under KSA § 60-467.

VI. THE FRE 403 WILDCARD.

A final determination on admissibility must address the test of Rule 403, balancing probative value against the dangers of unfair prejudice, confusion of the issues, misleading the jury, considerations of undue delay, waste of time, or the needless presentation of cumulative evidence. Some circumstances include:

1. When the evidence would contain offensive or highly derogatory language that may provoke an emotional response.
2. When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation.
3. When considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 1006.
4. In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence.

VII. PARTICULAR PROBLEMS WITH CERTAIN TYPES OF DATA.

Email

If you have a chain of emails, you should be prepared to authenticate and overcome hearsay objectives as to each ‘link in the chain.’

Emails stored by a business could be authenticated through testimony that the e-mails were stored in the ordinary course of business at or about the time the e-mail was sent, using trustworthy technology. *See* 7 Kan. L. & Prac. Handbook § 24:5.

Blogs

District of Kansas, in *Wilkins v. K-Mart Corp.*, sustained an objection to the admission of an article from particular website due to lack of foundation and stated that it would reconsider this ruling “if the plaintiff can come forward with expert testimony establishing a sufficient foundation.” 487 F. Supp. 2d 1216, 1223-24 (D. Kan. 2007).

Other jurisdictions hold that printouts from commercial websites are not self-authenticating. *See In re Carrsow-Franklin*, 456 B.R. 753, 756 (Bkr. D.S.C. 2011). Instead, “a witness declaration in combination with a document’s circumstantial indicia of authenticity (i.e., the date and web address that appear on [internet printouts])” constitutes a sufficient foundation. *Id.* at 756-57. For example, one Ninth Circuit case found printouts from a chat room admissible when the producer of the chat room logs testified as to how he created the logs and that the printouts appeared to be accurate representations, and there was an established connection between the Defendant and the chat room logs. *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000).

Some courts have created an extremely high burden for the authentication of internet printouts or the outright presumption that they are inadmissible:

“So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed.R.Civ.P. 807.”

St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999).

Social Media

“As with all evidence, the offering party must be prepared to demonstrate that the content from a social networking site is (1) relevant, (2) authentic, and (3) not subject to being excluded under the hearsay or best evidence rules.” John G. Browning, Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites, 14 SMU Sci. & Tech. L. Rev. 465, 478 (2011). The danger of social media evidence is that “[a]nyone can create a MySpace profile at no cost, . . . and can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password” Griffin v. State, 419 Md. 343, 351-52 (2011).

The seminal case in the authentication of website material is Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 548 (D. Md. 2007). Address the authentication of website postings, the Lorraine Court stated the following:

Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation. Their reaction has ranged from the famous skepticism expressed in *St. Clair v. Johnny's Oyster and Shrimp, Inc.* 76 F.Supp.2d 773 (S.D.Tex.1999),³⁰ to more permissive approach taken in *Perfect 10*, 213 F.Supp.2d at 1153-54.³¹

The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting. See *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir.2000) (excluding evidence of website postings because proponent failed to show that sponsoring organization actually posted the statements, as opposed to a third party); *St. Luke's*, 2006 WL 1320242 (plaintiff failed to authenticate exhibits of defendant's website postings

because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website); *Wady*, 216 F.Supp.2d 1060. One commentator has observed “[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (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?”³² The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

“The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data *556 has been republished by others who identify the source of the data as the website in question?”³³”

Counsel attempting to authenticate exhibits containing information from internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation. 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), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications).

Lorraine, 241 F.R.D. at 555-56.²

a. Methods for Authenticating Social Media Evidence

“The first, and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question, (i.e. [t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be.)” Griffin, 419 Md. at 363. “The second option may be to search the computer of the person who allegedly created the profile and posting and examine the computer’s internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question. Id. “A third method may be to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it.” Id. at 364.

Noting the “potential for abuse and manipulation of a social networking site by someone other than its purported creator,” the Griffin Court held that the MySpace posting should not have been admitted into evidence. Id. at 357-58. The Court stated that “a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of

²In its opinion, the court also addressed authentication issues related to e-mails, text messages and chat room content, computer stored records and data, computer animation and computer simulations, and digital photographs. Lorraine, 241 F.R.D. at 554-62.

the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the “snitches get stitches” language. Id. at 358

b. Additional Cases

In Massachusetts v. Williams, the Court held that testimony that the witness received instant messages on her MySpace page was insufficient evidence to authenticate the messages and they should not have been admitted. 456 Mass. 857, 869, 926 N.E.2d 1162, 1172 (2010). The Williams Court noted that

[a]lthough it appears that the sender of the messages was using [the defendant’s] MySpace Web “page,” there is no testimony . . . regarding how secure such a Web page is, who can access a Myspace Web page, whether codes are needed for such access, etc. Analogizing a Myspace Web page to a telephone call, a witness’s testimony that he or she has received an incoming call from a person claiming to be “A,” without more, is insufficient evidence to admit the call as a conversation with “A.”

Id. Further, the Court stated that “while the foundational testimony established that the messages were sent by someone with access to [the defendant’s] MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than [the defendant] could communicate from that Web page. Id. at 1172-73 (2010).

In Tienda v. Texas, the court concluded that MySpace postings could be authenticated with circumstantial evidence. PD-0312-11, 2012 WL 385381 (Tex. Crim. App. Feb. 8, 2012). The Tienda Court held that the combination of

“(1) the numerous photographs of the [defendant] with his unique arm, body, and neck tattoos, as well as his distinctive eyeglasses and earring; (2) the reference to [the victim’s death and the music from his funeral; (3) the references to [the defendant’s] gang; and (4) the messages referring to (a) a shooting at “Rumors” with “Nu-Nu,” (b) Hector as a “snitch,” and (c) the user having been on a monitor for a year (coupled with the photograph of the appellant lounging in a chair displaying an ankle monitor) sent from the MySpace pages of “ron Mr. T” or “MR. SMILEY FACE” whose email address is “ronnietiendajr@”—is sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the [defendant]. This is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the [defendant] and that he created and maintained them.

Id.

YouTube Videos

“The authentication of Skype, YouTube, and other video communications has not been a significant issue in litigation to date. It is likely that video communications will be treated for authentication purposes similarly to other video evidence and motion pictures; however, this is not certain yet. Generally, the courts treat videotape recordings and motion pictures like photographs for purposes of authentication.” 120 Am. Jur Proof of Facts 3d 93 § 8.

“Typically, the testimony of a witness who saw the fact, event, or circumstance in question, and who can verify that what was recorded is a fair and accurate representation of what occurred, will be sufficient to lay a foundation for admission of contemporaneous videotape evidence.” 16 Am. Jur. Proof of Facts 3d 493 § 10.

Could also be witness who did not witness the event depicted, but is familiar with general practices surrounding the recording. In *State v. Pham*, testimony of convenience store assistant manager that the store employed the use of security cameras, that security tapes were kept in an employees-only area, and that the tape from the security camera depicted the store at a certain time held to be sufficient foundation for introduction of photographic stills from security tape. 281 Kan. 1227, 1244-45 (2006).

VIII. HOW TO SUBPOENA FACEBOOK.

To Subpoena Facebook, you must send an email to Subpoena@facebook.com. There you will need to request instructions on how to subpoena information from Facebook. The company will likely provide you a manual. You will also want to attach your subpoena. The Facebook policy has been going through some changes, so you may want to request the company to provide you its most recent policy.

IX. WEBSITES TO OBTAIN INFORMATION ABOUT YOUR CLIENTS, OPPOSING PARTIES AND/OR JURORS.

The following websites can be used to obtain information about your clients, the opposing parties and/or jurors. These sites will provide information that may be useful in your cases. A good lawyer will also run his or her clients through the sites to see what information your client has posted on the web or see what other information might be out there on your client.

Spokeo.com
Pipl.com
Zabasearch.com

IX. CONCLUSIONS

The admissibility of ESI is evolving and a good trial lawyer will be prepared. Never assume that a photocopy of an email or other Electronic Evidence will be automatically admitted into evidence.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

H

United States District Court,
D. Maryland.
Jack R. LORRAINE and, Beverly Mack, Plaintiffs,
v.
MARKEL AMERICAN INSURANCE COMPANY,
Defendants.

Civil Action No. PWG-06-1893.
May 4, 2007.

Background: Suit was brought to enforce arbitrator's award. Parties moved and cross moved for summary judgment.

Holding: The District Court, Grimm, Chief United States Magistrate Judge, held that failure of both parties to observe evidence rules, as they applied to electronically stored information (ESI), precluded any entry of summary judgment.

Motions denied.

West Headnotes

[1] Alternative Dispute Resolution 25T 200

25T Alternative Dispute Resolution
25TII Arbitration
25TII(D) Performance, Breach, Enforcement,
and Contest
25Tk197 Matters to Be Determined by
Court
25Tk200 k. Arbitrability of Dispute.
Most Cited Cases

When the parties to an arbitration agreement do not agree to submit questions of arbitrability to the arbitrator for resolution, determining the scope of the agreement is an issue for the court to decide.

[2] Evidence 157 351

157 Evidence
157X Documentary Evidence

157X(C) Private Writings and Publications
157k351 k. Unofficial or Business Records
in General. Most Cited Cases

In order for electronically stored information (ESI) to be admissible, it must be (1) relevant, (2) authentic, (3) not hearsay or admissible under an exception to rule barring hearsay evidence, (4) original or duplicate, or admissible as secondary evidence to prove its contents, and (5) probative value must outweigh its prejudicial effect. Fed.Rules Evid.Rules 401, 403, 803, 804, 807, 901(a), 1001-1008, 28 U.S.C.A.

[3] Federal Civil Procedure 170A 2545

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2545 k. Admissibility. Most Cited Cases

Failure of counsel for both sides, in suit to compel arbitration, to observe evidence rules concerning electronically stored information (ESI), particularly rules governing authenticity, hearsay issues, original writing rule, and absence of unfair prejudice, rendered their summary judgment exhibits inadmissible. Fed.Rules Evid.Rules 401, 403, 803, 804, 807, 901(a), 1001-1008, 28 U.S.C.A.

*534 Geoffrey S. Tobias, Ober Kaler Grimes and Shriver, Baltimore, MD, for Plaintiffs.

Peter Joseph Basile, Ferguson Schetelich and Ballew PA, Baltimore, MD, for Defendant.

MEMORANDUM OPINION

GRIMM, Chief United States Magistrate Judge.

Plaintiffs/Counter-Defendants Jack Lorraine and Beverly Mack bring this action to enforce a private arbitrator's award finding that certain damage to their yacht, *Chessie*, was caused by a lightning strike that occurred on May 17, 2004, while *Chessie* was anchored in the Chesapeake Bay.^{EN1} Defendant/ Counter-Plaintiff Markel American Insurance Company

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

("Markel") likewise has counterclaimed to enforce the arbitrator's award, which, in addition to concluding that certain damage to *Chessie's* hull was caused by lightning, also concluded that the damage incurred was limited to an amount of \$14,100, plus incidental costs. Following discovery, Plaintiffs moved for summary judgment (Paper No. 16), and Defendants filed a response in opposition and cross motion for summary judgment (Paper No. 19), to which Plaintiffs filed an opposition and reply (Paper No. 21), followed by Defendant's reply (Paper No. 23). In a letter order dated February 7, 2007 (Paper No. 26), I denied without prejudice both motions for the reasons discussed more fully below, and informed the parties that I intended to file a more comprehensive opinion explaining my ruling, which is found herein.

FN1. This case has been referred to me for all proceedings with the consent of the parties. 28 U.S.C. § 636(c)(1)(2006); Local Rule 301.4.

BACKGROUND

It is difficult for the Court to provide the appropriate background to the underlying *535 arbitration in this case because, as will be discussed in greater detail below, neither party has proffered any admissible evidence to support the facts set forth in their respective motions. See FED.R.CIV.P. 56(c). Based on the pleadings, however, it appears undisputed that *Chessie* was struck by lightning on May 17, 2004, and that Plaintiffs filed a claim with Markel, their insurance carrier, for certain damage incurred as a result of the strike. Compl. ¶¶ 5, 6; Answer ¶¶ 2, 6. Markel issued payment under the policy for some of the damage claimed, and the matter would have been concluded had Plaintiffs not discovered damage to the hull when they pulled the boat out of the water several months later. Compl. ¶ 7. Markel denied that the hull damage was caused by the lightning strike and/or covered by Plaintiffs' insurance policy, and initiated a declaratory judgment action in the United States District Court for the Middle District of Pennsylvania to that effect. Compl. ¶ 13, Answer ¶ 15. The parties subsequently negotiated a private arbitration agreement and voluntarily dismissed the Pennsylvania claim. Compl. ¶ 15, Answer ¶ 17.

The scope of the arbitration agreement is the basis of this litigation. The final agreement states, in relevant part,

"The parties to this dispute ... have agreed that an arbitrator shall determine whether certain bottom damage in the amount of \$36,000, to the Yacht *CHESSIE* was caused by the lightning strike occurring on May 17, 2004, or osmosis, as claimed by [Markel]."

Pl.'s Mot. Ex. A, Def.'s Mot. Ex. C. The agreement also contemplated that the arbitrator would issue an "award" within 30 days of the final submission of evidence. *Id.* The arbitrator issued his award on June 12, 2006. In it, he held that some, but not all, of *Chessie's* hull damage was caused by lightning. Specifically, the arbitrator stated,

"I find that there *is* a basis for an argument regarding loss related damage. Evidence shows that the lightning strike on Mary 17, 2004 was discharged through the hull below the water line.... The **corruption of the surface laminate of the bottom** is basis for a loss related award.... The award amount must be kept in proportion to the **loss related damage** only. I find that the repairs relating to that damage should be based on a cost of \$300.00 per foot (\$14,000.00). Other expenses relating to charges for hauling, mast un-stepping/re-stepping, blocking, storage, moving, launching or environmental fees should be added to that amount."

Def.'s Mot. Ex. D. This award forms the basis for the present litigation, in which both parties ostensibly seek to confirm and enforce the arbitrator's decision.

SUMMARY JUDGMENT STANDARD

Summary judgment is appropriate when there exists no genuine issue as to any material fact and a decision may be rendered as a matter of law. Fed.R.Civ.P. 56(c); Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 247, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). The party moving for summary judgment has the burden of demonstrating that there are no genuine issues of material facts to resolve. Pulliam Inv. Co. v. Cameo Properties, 810 F.2d 1282, 1286 (4th Cir.1987). In determining whether summary judgment should be granted, the court "must assess the documentary materials submitted by the parties in the light most favorable to the nonmoving party." *Id.* (citing Gill v. Rollins Protective Services Co., 773 F.2d 592, 598 (4th Cir.1985)).

If the party seeking summary judgment demon-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

strates that there is no evidence to support the non-moving party's case, the burden shifts to the non-moving party to identify specific facts showing that there is a genuine issue for trial. The existence of only a "scintilla of evidence" is not enough to defeat a motion for summary judgment. Instead, the evidentiary materials submitted must show facts from which the finder of fact reasonably could find for the party opposing summary judgment. *Anderson*, 477 U.S. at 251, 106 S.Ct. 2505.

Moreover, to be entitled to consideration on summary judgment, the evidence supporting the facts set forth by the parties must be such as would be admissible in evidence. See *FED.R.CIV.P. 56(c)*; see also *Sakaria v. Trans World Airlines*, 8 F.3d 164, 171 (4th Cir.1993) (finding that the district court *536 properly did not consider inadmissible hearsay in an affidavit filed with motion for summary judgment); *Mitchell v. Data General Corp.*, 12 F.3d 1310, 1315-16 (4th Cir.1993) ("The summary judgment inquiry thus scrutinizes the plaintiff's case to determine whether the plaintiff has proffered sufficient proof in the form of admissible evidence that could carry the burden of proof in his claim at trial."). With regard to documentary evidence, this Court previously has held that,

"[u]nsworn, unauthenticated documents cannot be considered on a motion for summary judgment. To be admissible at the summary judgment stage, documents must be authenticated by and attached to an affidavit that meets the requirements of *Rule 56(e)*-that the documents be admissible in evidence."

Miskin v. Baxter Healthcare Corp. et al., 107 F.Supp.2d 669 (D.Md.1999) (Grimm, J.) (citing *Orsi v. Kirkwood*, 999 F.2d 86, 92 (4th Cir.1993)).

THE FEDERAL ARBITRATION ACT

As a preliminary matter, Plaintiffs have styled their complaint as one to enforce the arbitrator's award under § 9 of the Federal Arbitration Act, 9 U.S.C. § 1 et seq. (2006), when, in reality, it is a complaint to modify the award under section 10 of that statute. This is so because, although the arbitrator found that only \$14,100 of *Chessie's* hull damage was caused by lightning, Plaintiffs nonetheless ask the Court to award a judgment in the amount of \$36,000. Plaintiffs' argument regarding the substance of the agreement

between the parties further underscores this conclusion. Specifically, Plaintiffs allege that the parties entered into an "all or nothing" agreement, whereby the arbitrator was to determine that the hull damage was caused by lightning, and if so, award Plaintiffs the \$36,000.00 in damages claimed. Pl.'s MSJ at 5. According to Plaintiffs,

"the Arbitrator's sole function was to determine whether the hull damage, in the agreed-upon amount of \$36,000, was caused by the lightning strike occurring on May 17, 2004. *The Arbitration Agreement did not grant the Arbitrator the authority to assess a damage amount.*"

Id. (emphasis added). This argument is consistent with a motion to modify under § 10(b)(4), which permits a federal court to modify or vacate an arbitration award upon a showing that "the arbitrator[] exceeded their powers." Accordingly, the Court will evaluate Plaintiffs' motion under § 10 of the FAA.

In contrast, Markel's complaint truly is one to enforce the arbitrator's award. Markel denies that it entered into an "all or nothing" arbitration agreement with regard to damages, and seeks to enforce the arbitrator's award of \$14,100. Def.'s Mot. at 5.

The question before the Court, therefore, is whether the arbitrator exceeded his authority under the arbitration agreement by assigning a value to the damages attributable to the lightning strike that was less than the \$36,000 claimed by Plaintiffs. If the answer is yes, then the court can vacate, remand, or modify the award. 9 U.S.C. § 10, 11. If the answer is no, then the court must grant Defendant's motion to confirm the award under § 9 of the FAA.

[1] To resolve whether the arbitrator exceeded his authority, the Court first must determine the scope of the arbitration agreement; specifically, whether the parties agreed to arbitrate the amount of damages caused by the lightning strike. Because the parties did not agree to submit questions of arbitrability to the arbitrator for resolution, determining the scope of the agreement is an issue for the Court to decide. *First Options of Chicago, Inc. v. Kaplan*, 514 U.S. 938, 943, 115 S.Ct. 1920, 131 L.Ed.2d 985 (1995). In this regard, the Supreme Court has advised that, "[w]hen deciding whether the parties agreed to arbitrate a certain matter ... courts generally ... should apply ordinary

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

state-law principles of contract interpretation.” Kaplan, 514 U.S. at 944, 115 S.Ct. 1920, accord E.I. Dupont De Nemours & Co. v. Martinsville Nylon Employees’ Council Corp., 78 F.3d 578 (4th Cir.1996). In doing so, the Court must “give due regard to the federal policy favoring arbitration and resolve ‘any doubts concerning the scope of arbitrable issues in favor of arbitration.’ ” Hill v. PeopleSoft USA, Inc., 412 F.3d 540, 543 (4th Cir.2005) (quoting *537 Moses H. Cone Mem’l Hosp. v. Mercury Constr. Corp., 460 U.S. 1, 24-25, 103 S.Ct. 927, 74 L.Ed.2d 765 (1983)). Maryland law ^{FN2} regarding contract interpretation requires the court first to “determine from the language of the agreement itself what a reasonable person in the position of the parties would have meant at the time it was effectuated.” GMAC v. Daniels, 303 Md. 254, 262, 492 A.2d 1306, 1310 (Md.1985). If the language of the contract is clear and unambiguous, then the Court “must presume that the parties meant what they expressed.” Id. If the language of the contract is ambiguous, however, the court may consider parol evidence to determine the intent of the parties. E.g. Truck Ins. Exch. v. Marks Rentals, Inc., 288 Md. 428, 433, 418 A.2d 1187, 1190 (Md.1980). Contract language is ambiguous if it could be read to have more than one meaning by a reasonably prudent layperson. Clendenin Bros., Inc. v. United States Fire Ins. Co., 390 Md. 449, 459, 889 A.2d 387, 393-394 (Md.2006), citing Truck Ins. Exch., 288 Md. at 433, 418 A.2d at 1190.

^{FN2}. The parties do not dispute that Maryland law applies.

Here, I find that the language of the arbitration agreement is ambiguous; it could be read either to permit the arbitrator to determine the amount of damage to *Chessie*, or to limit his authority to determining only whether the claimed damages were caused by the lightning strike. Under normal circumstances, the Court would look to the documentary evidence provided by the parties, which in this case includes the arbitration agreement, award, and copies of e-mail correspondence between counsel, ostensibly supplied as extrinsic evidence of the parties’ intent with regard to the scope of the arbitration agreement. In this case, however, the admissibility problems with the evidence presented are manifest. First, none of the documentary evidence presented is authenticated by affidavit or otherwise. Next, most of the facts relevant to the contract negotiations at issue have been pro-

vided by counsel *ipse dixit*, without supporting affidavits or deposition testimony. The evidentiary problems associated with the copies of e-mail offered as parol evidence likewise are substantial because they were not authenticated, but instead were simply attached to the parties’ motions as exhibits.

Because neither party to this dispute complied with the requirements of Rule 56 that they support their motions with admissible evidence, I dismissed both motions without prejudice to allow resubmission with proper evidentiary support. (Paper No. 26). I further observed that the unauthenticated e-mails are a form of computer generated evidence that pose evidentiary issues that are highlighted by their electronic medium. Given the pervasiveness today of electronically prepared and stored records, as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence. Although cases abound regarding the discoverability of electronic records, research has failed to locate a comprehensive analysis of the many interrelated evidentiary issues associated with electronic evidence. Because there is a need for guidance to the bar regarding this subject, this opinion undertakes a broader and more detailed analysis of these issues than would be required simply to resolve the specific issues presented in this case. It is my hope that it will provide a helpful starting place for understanding the challenges associated with the admissibility of electronic evidence.

ADMISSIBILITY OF ELECTRONICALLY STORED INFORMATION

Be careful what you ask for, the saying goes, because you might actually get it. For the last several years there has been seemingly endless discussion of the rules regarding the discovery of electronically stored information (“ESI”). The adoption of a series of amendments to the Federal Rules of Civil Procedure relating to the discovery of ESI in December of 2006 has only heightened, not lessened, this discussion. Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes “such facts as would *538 be admissible in evidence” for use in summary judgment practice. FED.R.CIV.P. 56(e).^{FN3} This is unfortunate, because considering the significant costs associated with dis-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

covery 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. The process is complicated by the fact that ESI comes in multiple evidentiary “flavors,” including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files. ^{FN4}

^{FN3}. See, e.g. *Orsi v. Kirkwood*, 999 F.2d 86, 92 (4th Cir.1993) (“It is well established that unsworn, unauthenticated documents cannot be considered on a motion for summary judgment”); *Planmatics, Inc. v. Showers*, 137 F.Supp.2d 616, 620 (D.Md.2001) (“On a motion for summary judgment, a district court may only consider evidence that would be admissible at trial” (citations omitted)). See also *Maryland Highways Contractors Assoc., Inc. v. State of Maryland*, 933 F.2d 1246, 1251 (4th Cir.1991); *Wilson v. Clancy*, 747 F.Supp. 1154,1158 (D.Md.1990); JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN’S FEDERAL EVIDENCE § 901.02 [1] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997)(hereinafter “WEINSTEIN”).

^{FN4}. Examples of internet postings include; data posted by the site owner, data posted by others with the consent of the site owner, and data posted by others without consent, such as “hackers.” Examples of computer-generated documents and files include; electronically stored records or data, computer simulation, and computer animation. See 2 MCCORMICK ON EVIDENCE § 227 (John William Strong, et al. eds., 6th ed.2006); Gregory P. Joseph, *Internet and Email Evidence*, 13 PRAC. LITIGATOR (Mar.2002), reprinted in 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL, Part 4 at 20 (9th ed.2006)(hereinafter “Joseph”); Hon. Paul W. Grimm and Claudia Diamond, *Low-Tech Solutions to High-Tech Wizardry: Computer Generated Evidence*, 37 MD. B.J. 4 (July/August, 2004).

[2] Whether ESI is admissible into evidence is determined by a collection of evidence rules ^{FN5} 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, of 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. Preliminarily, the process by which the admissibility of ESI is determined is governed by Rule 104, which addresses the relationship between the judge and the jury with regard to preliminary fact finding associated with the admissibility of evidence. Because Rule 104 governs the very process of determining admissibility of ESI, it must be considered first.

^{FN5}. It has been noted that “[t]he Federal Rules of Evidence ... do not separately address the admissibility of electronic data.” ADAM COHEN AND DAVID LENDER, *ELECTRONIC DISCOVERY: LAW AND PRACTICE* § 6.01 (Aspen Publishers 2007). However, “the Federal Rules of Evidence apply to computerized data as they do to other types of evidence.” MANUAL FOR COMPLEX LITIGATION § 11.447 (4th ed.2004). Indeed, FED.R.EVID. 102 contemplates that the rules of evidence are flexible enough to accommodate future “growth and development” to address technical changes not in existence as of the codification of the rules themselves. Further, courts have had little difficulty using the existing rules of evidence to determine the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

admissibility of ESI, despite the technical challenges that sometimes must be overcome to do so. *See, e.g., In re F.P.*, 878 A.2d 91, 95 (Pa.Super.Ct.2005) (“Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages.... We believe that e-mail messages and similar forms of electronic communications can be properly authenticated within the existing framework of [the state rules of evidence].”).

***539 Preliminary Rulings on Admissibility(Rule 104)**

The relationship between Rule 104(a) and (b) can complicate the process by which ESI is admitted into evidence at trial, or may be considered at summary judgment. The rule states, in relevant part:

“(a) Questions of admissibility generally. Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b).... In making its determination it is not bound by the rules of evidence except those with respect to privileges.

(b) Relevancy conditioned on fact. When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.”

FED.R.EVID. 104(a) and (b).

When the judge makes a preliminary determination regarding the admissibility of evidence under Rule 104(a), the Federal Rules of Evidence, except for privilege, do not apply. Rule 104(a), 1101(d)(1). Therefore, the court may consider hearsay or other evidence that would not be admissible if offered to the jury,^{FN6} and “hearings on preliminary matters need not be conducted with all the formalities and requirements of a trial.”^{FN7} Accordingly, the trial judge may make preliminary determinations in chambers or at a sidebar conference in court.^{FN8}

FN6. Precision Piping and Instruments v. E.I. du Pont de Nemours and Co., 951 F.2d

613, 621 (4th Cir.1991); 1 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL, 104.03[1][b] (9th ed.2006)(hereinafter “SALTZBURG”); WEINSTEIN at § 104.11[1][a]; *Id.* at § 901.06[1][c][iii] (“Rule 104(a) provides that inadmissible evidence may be considered in determining preliminary questions of admissibility under Rule 104(a). However, that provision does not extend to determinations under Rule 104(b), so the court may not consider inadmissible evidence in determinations governed by Rule 104(b). In determining the preliminary question of authenticity under Rule 104(b), therefore, a judge may only consider evidence that is itself admissible.”).

FN7. WEINSTEIN at § 104.11[3].

FN8. Id.; United States v. Branch, 970 F.2d 1368 (4th Cir.1992).

The following types of preliminary matters typically are determined by the judge under Rule 104(a): whether an expert is qualified, and if so, whether his or her opinions are admissible; existence of a privilege; and whether evidence is hearsay, and if so, if any recognized exception applies.^{FN9}

FN9. WEINSTEIN at § 104.02[2].

The interplay between Rule 104(a) and 104(b) can be a bit tricky, which is illustrated by the manner in which evidence, whether ESI or “hard copy,” must be authenticated under Rule 901(a). Authentication under Rule 901 is viewed as a subset of relevancy, because “evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims.”^{FN10} Accordingly, “[r]esolution of whether evidence is authentic calls for a factual determination by the jury and admissibility, therefore, is governed by the procedure set forth in Federal Rule of Evidence 104(b) ‘relating to matters of conditional relevance generally.’ ”^{FN11} In essence, determining whether ESI is authentic, and therefore relevant, is a two step process. First, “[b]efore admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

evidence is authentic.”^{FN12} Then, “because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which *540 the proponent claims.”^{FN13} As the Fourth Circuit summarized this process:

FN10. Branch, 970 F.2d at 1370 (citing United States v. Sliker, 751 F.2d 477, 497-99 (2d Cir.1984)).

FN11. Id. (citation omitted). *See also, FED.R.EVID. 901(a)* advisory committee's notes (“Authentication and identification represent a special aspect of relevancy.... This requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b)”).

FN12. Branch, 970 F.2d at 1370 (citing FED.R.EVID. 104(b) advisory committee's note).

FN13. Id. at 1370-71.

“Although the district court is charged with making this preliminary determination, because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims. Because the ultimate resolution of authenticity is a question for the jury, in rendering its preliminary decision on whether the proponent of evidence has laid a sufficient foundation for admission the district court must necessarily assess the adequacy of the showing made before the jury.”^{FN14}

FN14. Id. (citation omitted)

With respect to this two step process, the Fourth Circuit went on to state:

“[a]n in camera hearing addressing authenticity does not replace the presentation of authenticating evidence before the jury; the district court must revisit this issue at trial. Thus, even though the district court may have ruled during an in camera pro-

ceeding that the proponent had presented sufficient evidence to support a finding that [the evidence] was authentic, evidence that would support the same ruling must be presented again, to the jury, before the [evidence] may be admitted.”^{FN15}

FN15. Id.

In short, there is a significant difference between the way that Rule 104(a) and 104(b) operate. Because, under Rule 104(b), the jury, not the court, makes the factual findings that determine admissibility, the facts introduced must be admissible under the rules of evidence.^{FN16} It is important to understand this relationship when seeking to admit ESI. 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 Rule 104(b), and the facts that they consider in making this determination must be admissible into evidence. In contrast, if the ruling on whether the e-mail is an admission by a party opponent or a business record turns on contested facts, the admissibility of those facts will be determined by the judge under 104(a), and the Federal Rules of Evidence, except for privilege, are inapplicable.

FN16. See, e.g., United States v. Safavian, 435 F.Supp.2d 36, 41-42 (D.D.C.2006) (trial judge relied on proffers of government lawyers about facts learned by FBI agents during their investigation to make preliminary determination that e-mails were admissible, but cautioned that at trial the government would have to call witnesses with personal knowledge of facts and not rely on FBI agents' testimony about what others had told them regarding the origin of the e-mails); SALTZBURG at § 901.02[5] (“In order for the trier of fact to make a rational decision as to authenticity [under Rule 104(b)], the foundation evidence must be admissible and it must actually be placed before the jury if the Judge admits the evidence”).

Relevance (Rules 401, 402, and 105)

The first evidentiary hurdle to overcome in establishing the admissibility of ESI is to demonstrate that it is relevant, as defined by Federal Rule of Evidence 401, which states:

“ ‘Relevant evidence’ means evidence having any

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.”

Clearly, facts that tend to prove essential elements of the causes of action and affirmative defenses asserted in the pleadings are “of consequence to the litigation,” as are facts that tend to undermine or rehabilitate the credibility of the witnesses who will testify. SALTZBURG at § 401.02[8]. So too, however, are background facts that, although they may not prove elements of the claims and defenses, and may not even be disputed, nonetheless routinely are admitted to help the fact finder understand the issues in the case and the evidence introduced to prove or disprove them. FED.R.EVID. 401 advisory committee's note. It is important to recognize that relevance is not a static concept; evidence is not relevant or irrelevant, occupying some rigid state of all or nothing. SALTZBURG at § 401.02[11]. Instead, “[r]elevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter *541 properly provable in the case.” FED.R.EVID. 401 advisory committee's note. As recognized by Federal Rule of Evidence 105, evidence may be admissible for one purpose, but not another, or against one party, but not another.^{FN17} Therefore, it is important for the proponent of the evidence to have considered all of the potential purposes for which it is offered, and to be prepared to articulate them to the court if the evidence is challenged. This point is particularly significant, as discussed below, when considering hearsay objections, where disputed evidence may be inadmissible hearsay if offered for its substantive truth, but admissible if offered for a reason other than its literal truth.

FN17. FED R. EVID. 105 states: “When evidence which is admissible as to one party or for one purpose but not admissible as to another party or for another purpose is admitted, the court, upon request, shall restrict the evidence to its proper scope and instruct the jury accordingly.”

In assessing whether evidence is relevant under Rule 401, it also is important to remember that there is a distinction between the admissibility of evidence, and the weight to which it is entitled in the eyes of the fact finder, as Rule 104(e)^{FN18} instructs. To be rele-

vant, evidence does not have to carry any particular weight—it is sufficient if it has “any tendency” to prove or disprove a consequential fact in the litigation. Whether evidence tends to make a consequential fact more probable than it would be without the evidence is not a difficult showing to make. FED.R.EVID. 401 advisory committee's note; SALTZBURG at § 401.02[1] (“To be relevant it is enough that the evidence has a *tendency* to make a consequential fact even the least bit more probable or less probable than it would be without the evidence. The question of relevance is thus different from whether the evidence is *sufficient* to prove a point.”) See also WEINSTEIN at § 401.05-06.

FN18. FED.R.EVID. 104(e) states: “[Rule 104] does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility [of evidence that has been admitted by an adverse party].”

The Federal Rules of Evidence are clear: evidence that is not relevant is never admissible. FED.R.EVID. 402. Once evidence has been shown to meet the low threshold of relevance, however, it presumptively is admissible unless the constitution, a statute, rule of evidence or procedure, or case law requires that it be excluded.^{FN19} Thus, the function of all the rules of evidence other than Rule 401 is to help determine whether evidence which in fact is relevant should nonetheless be excluded. FED.R.EVID. 402 advisory committee's note (“Succeeding rules [in Article IV of the rules of evidence] ... in response to the demands of particular policies, require the exclusion of evidence despite its relevancy.”). See also SALTZBURG § 402.02 [1]-[2].

FN19. Id. (stating that “[a]ll relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.”); SALTZBURG at § 401.02[1]; WEINSTEIN at § 402.02[1].

Establishing that ESI has some relevance generally is not hard for counsel. Articulating all of what may be multiple grounds of relevance is something that is important, though not as frequently done as it

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

should be. Accordingly, evidence that might otherwise be admitted may be excluded because the proponent put all his or her eggs in a single evidentiary basket, which the trial judge views as inapplicable, instead of carefully identifying each potential basis for admissibility. That was not the problem in this case, however, because the e-mail and other documentary evidence attached as exhibits to the summary judgment motions are relevant to determining the scope of the arbitration agreement between the parties, and therefore this evidence meets the requirements of Rule 401. Assuming, as is the case here, the proponent of ESI establishes its relevance and concomitant presumptive admissibility, the next step is to demonstrate that it is authentic. It is this latter step that the parties in this case omitted completely.

Authenticity (Rules 901-902)

In order for ESI to be admissible, it also must be shown to be authentic. Rule 901(a) defines what this entails: “[t]he requirement *542 of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.” As already noted, “[a]uthentication and identification represent a special aspect of relevancy.... This requirement of showing authenticity or identity falls into the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b).” FED.R.EVID. 901 advisory committee's note. The requirement of authentication and identification also insures that evidence is trustworthy, which is especially important in analyzing hearsay issues. Indeed, these two evidentiary concepts often are considered together when determining the admissibility of exhibits or documents.^{FN20} WEINSTEIN at § 901.02[2].

^{FN20}. See, e.g., In re Vee Vinhnee, 336 B.R. 437, 444 (9th Cir. BAP 2005) (In considering admissibility of electronically stored business records, the court noted “[o]rdinarily, because the business record foundation commonly covers the ground, the authenticity analysis [under Rule 902(11)] is merged into the business record analysis without formal focus on the question.” (citation omitted)).

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]. This is not a particularly high barrier to overcome. For example, in United States v. Safavian, 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.”

435 F.Supp.2d at 38 (citations omitted). See also United States v. Meienberg, 263 F.3d 1177, 1180 (10th Cir.2001) (analyzing admissibility of printouts of computerized records); United States v. Tank, 200 F.3d 627, 630 (9th Cir.2000) (analyzing admissibility of exhibits reflecting chat room conversations); United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir.1994)(discussing admissibility of radiotelegrams); United States v. Howard-Arias, 679 F.2d 363, 366 (4th Cir.1982)(addressing chain of authenticity); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 2004 WL 2367740, at * 16 (N.D.Ill. Oct.15, 2004) (analyzing admissibility of the content of a website).

Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation. See, e.g., In re Vee Vinhnee, 336 B.R. 437 (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 and Laser Institute PA 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); Rambus 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 and Accident Ins. Co. of Am., 216 F.Supp.2d 1060

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

(C.D.Cal.2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Assoc., 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).

Although courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication⁵⁴³ of "hard copy" documents,^{FN21} they have been quick to reject calls to abandon the existing rules of evidence when doing so. For example, in *In re F.P.* the court addressed the authentication required to introduce transcripts of instant message conversations. In rejecting the defendant's challenge to this evidence, it stated:

FN21. In *In re Vee Vinhnee*, 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...." 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." The court did conclude, however, that "it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground," before exercising a demanding analysis of the foundation needed to authenticate a paperless business record and lay the foundation for the business record exception to the hearsay rule, ultimately ruling that a proper foundation had not been established, and excluding the evidence. 336 B.R. at 444-45. See also MANUAL FOR COMPLEX LITIGATION at § 11.447 ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and

authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy. The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pre-trial proceedings, so that challenges to the evidence are not made for the first time at trial.").

"Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of PaR.E. 901 and Pennsylvania case law ... We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity."

878 A.2d at 95-96. Indeed, courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources. As one respected

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

commentator on the Federal Rules of Evidence has noted:

“In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.

***544** The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination. Factors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems. 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 processing.

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.”

WEINSTEIN at § 900.06[3]. Obviously, there is no “one size fits all” approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges.

Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished. It states:

“(b) Illustrations.

By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:

- (1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.
- (2) Nonexpert opinion on handwriting. Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.
- (3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.
- (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.
- (5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.
- (6) Telephone conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.
- (7) Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.
- (8) Ancient documents or data compilation. Evi-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

dence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) Methods provided by statute or rule. Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority.”

The ten methods identified by Rule 901(b) are non-exclusive. FED.R.EVID. 901(b) advisory committee's note (“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.”); WEINSTEIN at § 901.03[1] (“Parties may use any of the methods listed in Rule 901(b), any combination of them, or any other proof that may be available to carry their burden of showing that the proffered exhibit is what they claim it to be.”); Telewizja Polska USA, 2004 WL 2367740 (authentication methods listed in Rule 901(b) are “non-exhaustive”). 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).

Although the methods of authentication listed in Rule 901(b) “relate for the most part to documents ... some attention [has been] given to ... computer print-outs,” particularly Rule 901(b)(9), which was drafted with “recent developments” in computer technology in mind. FED.R.EVID. 901(b) advisory committee's note. When faced with resolving authentication issues for electronic evidence, courts have used a number of the methods discussed in Rule 901(b), as well as approved some methods not included in that rule:

Rule 901(b)(1).

This rule permits authentication by: “[t]estimony that a matter is what it is claimed to be.” This rule

“contemplates a broad spectrum” including “testimony of a witness who was present at the signing of a document....” FED.R.EVID. 901(a) advisory committee's note. “[I]n recognition of the proponent's light burden of proof in authenticating an exhibit ... the ‘knowledge’ requirement of Rule 901(b)(1) is liberally construed. A witness may be appropriately knowledgeable through having participated in or observed the event reflected by the exhibit.” WEINSTEIN at § 901.03[2] (cross-reference omitted). Courts considering the admissibility of electronic evidence frequently have acknowledged that it may be authenticated by a witness with personal knowledge. United States v. Kassimu, 2006 WL 1880335 (5th Cir. May 12, 2006) (ruling that copies of a post office's computer records could be authenticated by a custodian or other qualified witness with personal knowledge of the procedure that generated the records); St. Luke's, 2006 WL 1320242 at *3-4 (“To authenticate printouts from a website, the party proffering the evidence must produce ‘some statement or affidavit from someone with knowledge [of the website] ... for example [a] web master or someone else with personal knowledge would be sufficient.’” (citation omitted)); Safavian, 435 F.Supp.2d at 40 n. 2 (D.D.C.2006) (noting that e-mail may be authenticated by a witness with knowledge that the exhibit is what it is claimed to be); Wady, 216 F.Supp.2d 1060 (sustaining objection to affidavit of plaintiff's witness attempting to authenticate documents taken from the defendant's website because the affiant lacked personal knowledge of who maintained the website or authored the documents). Although Rule 901(b)(1) certainly is met by the testimony of a witness that actually drafted the exhibit, it is not required that the authenticating witness have personal knowledge of the making of a particular exhibit if he or she has personal knowledge of how that type of exhibit is routinely made. WEINSTEIN at § 901.03[2].^{FN22} It is necessary, however, that the authenticating witness provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business record*546 exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8).

^{FN22}. “Offentimes a witness need not be familiar with specific exhibits to be suffi-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

ciently knowledgeable to authenticate or identify them. Business records and records of government agencies, for example, are frequently authenticated by witnesses who have never seen the specific records that comprise the exhibits and know nothing about the specific information they contain. Their authentication is accomplished when a witness identifies the exhibits as documents of a type that the organization typically develops, and testifies about the procedures the organization follows in generating, acquiring, and maintaining documents of that type, and explains the method by which the specific exhibits were retrieved from the organization's files. Similarly, exhibits that are automatically produced upon the occurrence of specified events may be authenticated by the testimony of persons with knowledge of the system or process that results in the production of the exhibit." (footnote omitted).

Rule 901(b)(3).

This rule allows authentication or identification by "[c]omparison by the trier of fact or by expert witnesses with specimens which have been authenticated." Interestingly, the rule allows either expert opinion testimony to authenticate a questioned document by comparing it to one known to be authentic, or by permitting the factfinder to do so. Obviously, the specimen used for the comparison with the document to be authenticated must be shown itself to be authentic. WEINSTEIN at § 901.03[7][b]. This may be accomplished by any means allowable by Rule 901 or 902, as well as by using other exhibits already admitted into evidence at trial, or admitted into evidence by judicial notice under Rule 201. *Id.* Although the common law origin of Rule 901(b)(3) involved its use for authenticating handwriting or signatures, FED. R. EVID. 901(b)(3) advisory committee's note, it now is commonly used to authenticate documents, WEINSTEIN at § 901.03[7][b], and at least one court has noted its appropriate use for authenticating e-mail. Safavian, 435 F.Supp.2d at 40 (E-mail messages "that are not clearly identifiable on their own can be authenticated ... by comparison by the trier of fact (the jury) with 'specimens which have been [otherwise] authenticated'-in this case, those e-mails that already have been independently authenticated under Rule 901(b)(4).").

Rule 901(b)(4).

This rule is one of the most frequently used to authenticate e-mail and other electronic records. It permits exhibits to be authenticated or identified by "[a]pppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." The commentary to Rule 901(b)(4) observes "[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety," including authenticating an exhibit by showing that it came from a "particular person by virtue of its disclosing knowledge of facts known peculiarly to him," or authenticating "by content and circumstances indicating it was in reply to a duly authenticated" document. FED.R.EVID. 901(b)(4) advisory committee's note. Use of this rule often is characterized as authentication solely by "circumstantial evidence." WEINSTEIN at § 901.03[8]. Courts have recognized this rule as a means to authenticate ESI, including e-mail, text messages and the content of websites. *See United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir.2000) (allowing the authentication of an e-mail entirely by circumstantial evidence, including the presence of the defendant's work e-mail address, content of which the defendant was familiar with, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the e-mail); Safavian, 435 F.Supp.2d at 40 (same result regarding e-mail); *In re F.P.*, 878 A.2d at 94 (noting that authentication could be accomplished by direct evidence, circumstantial evidence, or both, but ultimately holding that transcripts of instant messaging conversation circumstantially were authenticated based on presence of defendant's screen name, use of defendant's first name, and content of threatening message, which other witnesses had corroborated); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1153-54 (C.D.Cal.2002) (admitting website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses).

One method of authenticating electronic evidence under Rule 901(b)(4) is the use of "hash values" or "hash marks" when making documents. A hash value is:

"A unique numerical identifier that can be assigned

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. ‘Hashing’ is used to guarantee the authenticity of an original data set and can be used as a digital *547 equivalent of the Bates stamp used in paper document production.^{FN23}

^{FN23.} Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, Federal Judicial Center, 2007 at 24; see also *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 655 (D.Kan.2005).

Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4). Also, they can be used during discovery of electronic records to create a form of electronic “Bates stamp” that will help establish the document as electronic.^{FN24} This underscores a point that counsel often overlook. A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the “final” or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. Use of hash values when creating the “final” or “legally operative” version of an electronic record can insert distinctive characteristics into that allow its authentication under Rule 901(b)(4).

^{FN24.} See, e.g., United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 20, <http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf> (last visited April 10, 2007) (encouraging parties to discuss use of hash values or “hash marks” when producing electronic records in dis-

covery to facilitate their authentication).

Another way in which electronic evidence may be authenticated under Rule 901(b)(4) is by examining the metadata for the evidence. Metadata,

“commonly described as ‘data about data,’ is defined as ‘information describing the history, tracking, or management of an electronic document.’ Appendix F to *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* defines metadata as ‘information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).’ Technical Appendix E to the *Sedona Guidelines* provides an extended description of metadata. It further defines metadata to include ‘all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records.’ Some examples of metadata for electronic documents include: a file’s name, a file’s location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept.”

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. at 646 (footnote omitted); Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, Federal Judicial Center, 2007 at 24-25 (defining metadata as “[i]nformation about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified ...”). Recently revised Federal Rule of Civil Procedure 34 permits a party to discover electronically stored information and to identify the form or forms in which it is to be produced. A party therefore can request production of electronically stored information in its “native format”, which includes the metadata for the electronic document.^{FN25} Because metadata shows

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

the date, *548 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 electronic evidence that can be used to authenticate it under Rule 901(b)(4). Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because,

FN25. United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 17, [http:// www. m dd.uscourts.gov/news/news/ESIProtocol.pdf](http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf) (last visited April 10, 2007) (“When parties have agreed or the Court has ordered the parties to exchange all or some documents as electronic files in Native File format in connection with discovery, the parties should collect and produce said relevant files in Native File formats in a manner that preserves the integrity of the files, including, but not limited to the contents of the file, the Meta-Data (including System Meta-Data, Substantive Meta-Data, and Embedded Meta-Data....”).

“[a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide for a selected network administrators to override an individual password identification number to gain access when necessary.”

WEINSTEIN at § 900.01[4][a]; see also *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 530 (1 st Cir.1996) (discussing how metadata markers can reflect that a document was modified when in fact it simply was saved to a different location). Despite its lack of conclusiveness, however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics.

Rule 901(b)(7):

This Rule permits authentication by:

“Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported

public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.”

The commentary to Rule 901(b)(7) recognizes that it applies to computerized public records, noting that “[p]ublic records are regularly authenticated by proof of custody, without more. [Rule 901(b)(7)] extends the principle to include data stored in computers and similar methods, of which increasing use in the public records area may be expected.” FED.R.EVID. 901(b)(7) advisory committee’s note (citation omitted). To use this rule the “proponent of the evidence need only show that the office from which the records were taken is the legal custodian of the records.” WEINSTEIN at § 901.10[2]. This may be done by “[a] certificate of authenticity from the public office; [t]he testimony of an officer who is authorized to attest to custodianship, [or] the testimony of a witness with knowledge that the evidence is in fact from a public office authorized to keep such a record.” *Id.* (footnote omitted). Examples of the types of public records that may be authenticated by Rule 901(b)(7) include tax returns, weather bureau records, military records, social security records, INS records, VA records, official records from federal, state and local agencies, judicial records, correctional records, law enforcement records, and data compilations, which may include computer stored records. *Id.*

Courts have recognized the appropriateness of authenticating computer stored public records under Rule 901(b)(7) as well, and observed that under this rule, unlike Rule 901(b)(9), there is no need to show that the computer system producing the public records was reliable or the records accurate. For example, in *United States v. Meienberg*, the court rejected defendant’s challenge to the admissibility of a law enforcement agency’s computerized records. Defendant argued that the only way they could be authenticated was under Rule 901(b)(9), through proof that they were produced by a system or process capable of producing a reliable result. Defendant further argued that the records had not been shown to be accurate. The appellate court disagreed, holding that the records properly had been authenticated under Rule 901(b)(7), which did not require a showing of accuracy. The court noted that any question regarding the accuracy of the records went to weight rather than admissibility. 263 F.3d at 1181. Thus, a decision to authenticate under Rule 901(b)(7), as opposed to 901(b)(9) may

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

mean that the required foundation is much easier to prove. *549 This underscores the importance of the point previously made, that there may be multiple ways to authenticate a particular computerized record, and careful attention to all the possibilities may reveal a method that significantly eases the burden of authentication.

Rule 901(b)(9):

This Rule recognizes one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. It authorizes authentication by “[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.” FED.R.EVID. 901(b)(9). This rule was “designed for situations in which the accuracy of a result is dependent upon a process or system which produces it.” FED.R.EVID. 901(b)(9) advisory committee’s note. See also WEINSTEIN at § 901.12[3]; ^{FN26} *In re Vee Vinhnee*, 336 B.R. at 446 (“Rule 901(b)(9), which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. The advisory committee note makes plain that Rule 901(b)(9) was designed to encompass computer-generated evidence ...”). ^{FN27}

^{FN26}. “Computer output may be authenticated under Rule 901(b)(9)... When the proponent relies on the provisions of Rule 901(b)(9) instead of qualifying the computer-generated information for a hearsay exception, it is common for the proponent to provide evidence of the input procedures and their accuracy, and evidence that the computer was regularly tested for programming errors. At a minimum, the proponent should present evidence sufficient to warrant a finding that the information is trustworthy and provide the opponent with an opportunity to inquire into the accuracy of the computer and of the input procedures.”

^{FN27}. In *Vinhnee*, the court cited with approval an eleven-step foundational authentication for computer records advocated by one respected academic. *Id.* (citing EDWARD J. IMWINKELRIED, EVIDEN-

TIARY FOUNDATIONS 58-59 (LexisNexis 6th ed.2005)). Although this foundation is elaborate, and many courts might not be so demanding as to require that it be followed to authenticate computer generated records, the fact that one court already has done so should put prudent counsel on notice that they must pay attention to how they will authenticate computer generated records, and that they should be prepared to do so in a manner that complies with the Federal Rules of Evidence and any governing precedent. The price for failing to do so may be, as in *In re Vee Vinhnee*, exclusion of the exhibit. See, e.g., *Indianapolis Minority Contractors Ass’n, Inc. v. Wiley*, 1998 WL 1988826, at *7 (S.D.Ind. May 13, 1998) (“[A]s a condition precedent to admissibility of computer records, the proponent must establish that the process or system used produces an accurate result, FED.R.EVID. 901(b)(9), and that foundation has not been established. In light of the above, the veracity and reliability of these reports are questionable, and thus [the summary judgment exhibit] will be stricken”).

Rule 902:

In addition to the non-exclusive methods of authentication identified in Rule 901(b), Rule 902 identifies twelve methods by which documents, including electronic ones, may be authenticated without extrinsic evidence. This is commonly referred to as “self-authentication.” The rule states:

“Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

- (1) Domestic public documents under seal. A document bearing a seal purporting to be that of the United States, or of any State, district, Commonwealth, territory, or insular possession thereof, or the Panama Canal Zone, or the Trust Territory of the Pacific Islands, or of a political subdivision, department, officer, or agency thereof, and a signature purporting to be an attestation or execution.
- (2) Domestic public documents not under seal. A document purporting to bear the signature in the official capacity of an officer or employee of any entity included in paragraph (1) hereof, having no

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

seal, if a public officer having a seal and having official duties in the district or political subdivision of the officer or employee certifies under seal that the signer has the official capacity and that the signature is genuine.

(3) Foreign public documents. A document purporting to be executed or attested in an official capacity by a person authorized by the laws of a foreign country to make the execution or attestation, and accompanied by a final certification as to the genuineness of the signature and official position (A) of the executing or attesting person, or (B) of any foreign official whose certificate of genuineness of signature and official position relates to the execution or attestation or is in a chain of certificates of genuineness of signature and official position relating to the execution or attestation. A final certification may be made by a secretary of an embassy or legation, consul general, consul, vice consul, or consular agent of the United States, or a diplomatic or consular official of the foreign country assigned or accredited to the United States. If reasonable opportunity has been given to all parties to investigate the authenticity and accuracy of official documents, the court may, for good cause shown, order that they be treated as presumptively authentic without final certification or permit them to be evidenced by an attested summary with or without final certification.

(4) Certified copies of public records. A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.

(6) Newspapers and periodicals. Printed materials purporting to be newspapers or periodicals.

(7) Trade inscriptions and the like. Inscriptions,

signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.

(8) Acknowledged documents. Documents accompanied by a certificate of acknowledgment executed in the manner provided by law by a notary public or other officer authorized by law to take acknowledgments.

(9) Commercial paper and related documents. Commercial paper, signatures thereon, and documents relating thereto to the extent provided by general commercial law.

(10) Presumptions under Acts of Congress. Any signature, document, or other matter declared by Act of Congress to be presumptively or prima facie genuine or authentic.

(11) Certified domestic records of regularly conducted activity. 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.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

(12) Certified foreign records of regularly con-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

ducted activity. In a civil case, the original or a duplicate of a foreign record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration by its custodian or other qualified person 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;

*551 (B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

The declaration must be signed in a manner that, if falsely made, would subject the maker to criminal penalty under the laws of the country where the declaration is signed. A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.”

The obvious advantage of Rule 902 is that it does not require the sponsoring testimony of any witness to authenticate the exhibit-its admissibility is determined simply by examining the evidence itself, along with any accompanying written declaration or certificate required by Rule 902. The mere fact that the rule permits self-authentication, however, does not foreclose the opposing party from challenging the authenticity. Because Rule 104(b) applies in such cases, the exhibit and the evidence challenging its authenticity goes to the jury, which ultimately determines whether it is authentic. FED.R.EVID. 902 advisory committee's note. Some of the examples contained in Rule 902, such as Rule 902(3) (foreign public documents), 902(4) (certified copies of public records), 902(8) (acknowledged documents), 902(11) (certified copies of domestic records of a regularly conducted activity), and 902(12) (certified foreign records of regularly conducted activity), do require a certificate signed by a custodian or other qualified person to accomplish the self-authentication.

Although all of the examples contained in Rule 902 could be applicable to computerized records, three in particular have been recognized by the courts to authenticate electronic evidence: 902(5) (official publications); 902(7) (trade inscriptions); and, 902(11) (certified domestic records of regularly conducted activity). The first, Rule 902(5), provides:

“(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.”

The rule “[dispenses] with preliminary proof of the genuineness of purportedly official publications [but] does not confer admissibility upon all official publications; it merely provides a means whereby their authenticity may be taken as established for purposes of admissibility.” FED.R.EVID. 902(5) advisory committee's note. This means that, to be admissible, the proponent may also need to establish that the official record qualifies as a public record hearsay exception under Rule 803(8). WEINSTEIN at § 902.02[2]. Although the rule is silent regarding the level of government that must authorize the publication, commentators suggest that the list includes the United States, any State, district, commonwealth, territory or insular possession of the United States, the Panama Canal Zone, the Trust Territory of the Pacific islands, or a political subdivision, department, officer, or agency of any of the foregoing. *Id.*

In Equal Employment Opportunity Commission v. E.I. DuPont de Nemours and Co., the court admitted into evidence printouts of postings on the website of the United States Census Bureau as self-authenticating under Rule 902(5). 2004 WL 2347556 (E.D.La. Oct.18, 2004). Given the frequency with which official publications from government agencies are relevant to litigation and the increasing tendency for such agencies to have their own websites, Rule 902(5) provides a very useful method of authenticating these publications. When combined with the public records exception to the hearsay rule, Rule 803(8), these official publications posted on government agency websites should be admitted into evidence easily.

Rule 902(7) provides that exhibits may be self-authenticated by “[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.” As one commentator has noted, “[u]nder Rule 902(7),

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the *552 employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7).” WEINSTEIN at § 900.07[3][c].

Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness to testify in person at trial. It provides:

“(11) Certified domestic records of regularly conducted activity. 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.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.”

This rule was added in the 2000 amendments to the Federal Rules of Evidence, and it was intended to “[set] forth a procedure by which parties can authenticate certain records of regularly conducted activity, other than through the testimony of a foundation witness.” FED.R.EVID. 902(11) advisory committee’s note. Unlike most of the other authentication rules,

Rule 902(11) also contains a notice provision, requiring the proponent to provide written notice of the intention to use the rule to all adverse parties and to make available to them the records sufficiently in advance of litigation to permit a fair opportunity to challenge them. WEINSTEIN at § 902.13[2]. Because compliance with Rule 902(11) requires the proponent to establish all the elements of the business record exception to the hearsay rule, Rule 803(6), courts usually analyze the authenticity issue under Rule 902(11) concomitantly with the business record hearsay exception.^{FN28} Rambus, 348 F.Supp.2d at 701 (“Thus, the most appropriate way to view Rule 902(11) is as the functional equivalent of testimony offered to authenticate a business record tendered under Rule 803(6) because the declaration permitted by Rule 902(11) serves the same purpose as authenticating testimony ... [B]ecause Rule 902(11) contains the same requirements, and almost the same wording, as Rule 803(6), decisions explaining the parallel provisions of Rule 803(6) are helpful in resolving the issues here presented.”); In re Vee Vinhnee, 336 B.R. at 444 (stating that in deciding whether to admit business records, the authenticity analysis is merged into the business record analysis).

^{FN28}. Because the business record exception will be discussed at some length below, the analysis of the requirements of Rule 902(11) will be deferred until that discussion.

Finally, as noted at the beginning of this discussion regarding the authenticating electronic records, Rule 901(b) makes clear that the ten examples listed are illustrative only, not exhaustive. In ruling on whether electronic evidence has been properly authenticated, courts have been willing to think “outside of the box” to recognize new ways of authentication. For example, they have held that documents provided to a party during discovery by an opposing party are presumed to be authentic, shifting the burden to the producing party to demonstrate that the evidence that they produced was not authentic. Indianapolis Minority Contractors Ass’n, 1998 WL 1988826, at *6 (“The act of production is an implicit authentication of documents produced.... Federal Rule of Evidence 901 provides that “[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. Defendants admit that they did produce [the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

exhibits at issue].... Thus ... the *553 Defendants cannot have it both ways. They cannot voluntarily produce documents and implicitly represent their authenticity and then contend they cannot be used by the Plaintiffs because the authenticity is lacking.” (citation omitted); *Perfect 10*, 213 F.Supp.2d at 1153-54 (finding that exhibits of website postings had been properly authenticated for three reasons, including that certain of them had been provided to the plaintiff by the defendant during discovery).

In *Telewizja Polska USA*, the court embraced a non-traditional method of authentication when faced with determining whether exhibits depicting the content of the defendant's website at various dates several years in the past were admissible. 2004 WL 2367740. The plaintiff offered an affidavit from a representative of the Internet Archive Company, which retrieved copies of the defendant's website as it appeared at relevant dates to the litigation through use of its “wayback machine.”^{FN29} The defendant objected, contending that the Internet Archive was not a reliable source, and thus the exhibits had not been authenticated. The court disagreed, stating:

^{FN29}. The “wayback machine” refers to the process used by the Internet Archive Company, www.archive.org, to allow website visitors to search for archived web pages of organizations. *St. Luke's*, 2006 WL 1320242 at *1.

“Federal Rule of Evidence 901 ‘requires only a prima facie showing of genuineness and leaves it to the jury to decide the true authenticity and probative value of the evidence.’ Admittedly, the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in Rule 901; the Internet Archive is a relatively new source for archiving websites. Nevertheless, Plaintiff has presented no evidence that the Internet Archive is unreliable or biased. And Plaintiff has neither denied that the exhibit represents the contents of its website on the dates in question, nor come forward with its own evidence challenging the veracity of the exhibit. Under these circumstances, the Court is of the opinion that [the affidavit from the representative of the Internet Archive Company] is sufficient to satisfy Rule 901's threshold requirement for admissibility.”

Id. at *6.

Additionally, authentication may be accomplished by the court taking judicial notice under Rule 201 of certain foundational facts needed to authenticate an electronic record. Under this rule, the parties may request the court to take judicial notice of adjudicative facts that are either (1) generally known within the territorial jurisdiction of the trial court, or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. FED.R.EVID. 201(b); WEINSTEIN at § 201.12[1]. Judicial notice could be a helpful way to establish certain well known characteristics of computers, how the internet works, scientific principles underlying calculations performed within computer programs, and many similar facts that could facilitate authenticating electronic evidence.

Authentication also can be accomplished in civil cases by taking advantage of FED.R.CIV.P. 36, which permits a party to request that his or her opponent admit the “genuineness of documents.” Also, at a pretrial conference, pursuant to FED.R.CIV.P. 16(c)(3), a party may request that an opposing party agree to stipulate “regarding the authenticity of documents,” and the court may take “appropriate action” regarding that request. Similarly, if a party properly makes his or her FED. R. CIV. P. 26(a)(3) pretrial disclosures of documents and exhibits, then the other side has fourteen days in which to file objections. Failure to do so waives all objections other than under Rules 402 or 403, unless the court excuses the waiver for good cause. This means that if the opposing party does not raise authenticity objections within the fourteen days, they are waived.

The above discussion underscores the need for counsel to be creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in Rules 901 and 902 that neatly fits.

Finally, any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the *554 wide diversity of such evidence, there is no single approach to authentication that will work in all instances. It is possible, however, to identify certain authentication issues that have been noted by courts and commentators with

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

particular types of electronic evidence and to be forearmed with this knowledge to develop authenticating facts that address these concerns.

E-mail

There is no form of ESI more ubiquitous than e-mail, and it is the category of ESI at issue in this case. Although courts today have more or less resigned themselves to the fact that “[w]e live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation’s population, and is of particular importance in the professional world,” *Safavian*, 435 F.Supp.2d at 41, it was not very long ago that they took a contrary view—“[e]-mail is far less of a systematic business activity than a monthly inventory printout.” *Monotype Corp. PLC v. Int’l Typeface*, 43 F.3d 443, 450 (9th Cir.1994) (affirming trial court’s exclusion of e-mail as inadmissible as a business record). Perhaps because of the spontaneity and informality of e-mail, people tend to reveal more of themselves, for better or worse, than in other more deliberative forms of written communication. For that reason, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved. Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence. See, e.g., *Safavian*, 435 F.Supp.2d 36.

Not surprisingly, there are many ways in which e-mail evidence may be authenticated. One well respected commentator has observed:

“[E]-mail messages may be authenticated by direct or circumstantial evidence. An e-mail message’s distinctive characteristics, including its ‘contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances’ may be sufficient for authentication.

Printouts of e-mail messages ordinarily bear the sender’s e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer’s reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender’s listed e-mail address.

The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message.

E-mails may even be self-authenticating. Under Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7). However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner’s name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.”

WEINSTEIN at § 900.07[3][c]; see also EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[4][b] (LexisNexis 6th ed.2005)(hereinafter “IMWINKELRIED, EVIDENTIARY FOUNDATIONS.”) Courts also have approved the authentication of e-mail by the above described methods. See, e.g., *Siddiqui*, 235 F.3d at 1322-23 (E-mail may be authenticated entirely by circumstantial evidence, including its distinctive characteristics); *Safavian*, 435 F.Supp.2d at 40 (recognizing that e-mail may be authenticated by distinctive characteristics 901(b)(4), or by comparison of exemplars with other e-mails that already have been authenticated 901(b)(3)); *Rambus*, 348 F.Supp.2d 698 (E-mail that qualifies as business record may be *555 self-authenticating under 902(11)); *In re F.P.*, 878 A.2d at 94 (E-mail may be authenticated by direct or circumstantial evidence).

The most frequent ways to authenticate e-mail evidence are 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).

Internet Website Postings

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation. Their reaction has ranged from the famous skepticism expressed in *St. Clair v. Johnny's Oyster and Shrimp, Inc.* 76 F.Supp.2d 773 (S.D.Tex.1999),^{FN30} to more permissive approach taken in *Perfect 10*, 213 F.Supp.2d at 1153-54.^{FN31}

^{FN30}. There, the court stated that,

“Plaintiff’s electronic ‘evidence’ is totally insufficient to withstand Defendant’s Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant’s Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in FED.R.EVID. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form from the United States Coast Guard or discover alternative information verifying what Plaintiff alleges.”

Id. at 774-775.

^{FN31}. The court noted that a “reduced evi-

dentiary standard” applied to the authentication of exhibits purporting to depict the defendant’s website postings during a preliminary injunction motion. The court found that the exhibits had been authenticated because of circumstantial indicia of authenticity, a failure of the defendant to deny their authenticity, and the fact that the exhibits had been produced in discovery by the defendant. The court declined to require proof that the postings had been done by the defendant or with its authority, or evidence to disprove the possibility that the contents had been altered by third parties.

The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting. See *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir.2000) (excluding evidence of website postings because proponent failed to show that sponsoring organization actually posted the statements, as opposed to a third party); *St. Luke’s*, 2006 WL 1320242 (plaintiff failed to authenticate exhibits of defendant’s website postings because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website); *Wady*, 216 F.Supp.2d 1060. One commentator has observed “[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (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?”^{FN32} The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

^{FN32}. Joseph at 21; see also SALTZBURG at § 901.02[12].

“The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

data, in whole or in part; whether others have published the same data, in whole or in part; whether the data *556 has been republished by others who identify the source of the data as the website in question? ^{FN33,}

FN33. *Id.* at 22.

Counsel attempting to authenticate exhibits containing information from internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation. 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), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications).

Text Messages and Chat Room Content

Many of the same foundational issues found encountered when authenticating website evidence apply with equal force to text messages and internet chat room content; however, 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 rooms was posted with the knowledge or authority of the website host. SALTZBURG at § 901.02[12]. One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

“(1) [e]vidence 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]; evidence 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].”

Id. at § 901.02[12]. Courts also have recognized that exhibits of chat room conversations may be au-

thenticated circumstantially. For example, in *In re F.P.*, the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. 878 A.2d at 93-94. The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts. *Id.* Similarly, in *United States v. Simpson*, the court held that there was ample circumstantial evidence to authenticate printouts of the content of chat room discussions between the defendant and an undercover detective, including use of the e-mail name of the defendant, the presence of the defendant's correct address in the messages, and notes seized at the defendant's home containing the address, e-mail address and telephone number given by the undercover officer. 152 F.3d at 1249. Likewise, in *United States v. Tank*, the court found sufficient circumstantial facts to authenticate chat room conversations, despite the fact that certain portions of the text of the messages in which the defendant had participated had been deleted. 200 F.3d at 629-31. There, the court found the testimony regarding the limited nature of the deletions by the member of the chat room club who had made the deletions, circumstantial evidence connecting the defendant to the chat room, including the use of the defendant's screen name in the messages, were sufficient to authenticate the messages. *Id.* at 631. Based on the foregoing cases, the rules most likely to be used to authenticate chat room and text messages, alone or in combination, appear to be 901(b)(1) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics).

Computer Stored Records and Data

Given the widespread use of computers, there is an almost limitless variety of records that are stored in or generated by computers. As one commentator has observed “[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 *557 of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements.” WEINSTEIN at § 900.06[3]. The least complex admissibility issues are associated with electronically stored records. “In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues.” WEINSTEIN at §

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

900.06[3]. That said, although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional “hard copy” records. MANUAL FOR COMPLEX LITIGATION at § 11.447; ^{FN34} see also IMWINKELRIED, EVIDENTIARY FOUNDATIONS at 4.03[2].^{FN35}

^{FN34}. “Computerized data”, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.

“The judge should therefore consider the accuracy and reliability of computerized evidence....”

^{FN35}. “In the past, many courts have been lax in applying the authentication requirement to computer records; they have been content with foundational evidence that the business has successfully used the computer system in question and that the witness recognizes the record as output from the computer. However, following the recommendations of the Federal Judicial Center’s *Manual for Complex Litigation*, some courts now require more extensive foundation. 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.” (citation omitted).

Two cases illustrate the contrast between the more lenient approach to admissibility of computer records and the more demanding one. In *United States v. Meienberg*, the defendant challenged on appeal the

admission into evidence of printouts of computerized records of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records. 263 F.3d at 1180-81. The Tenth Circuit disagreed, stating:

“Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility.”

Id. at 1181 (citation omitted). See also *Kassimu*, 2006 WL 1880335 (To authenticate computer records as business records did not require the maker, or even a custodian of the record, only a witness qualified to explain the record keeping system of the organization to confirm that the requirements of Rule 803(6) had been met, and the inability of a witness to attest to the accuracy of the information entered into the computer did not preclude admissibility); *Sea-Land Serv., Inc. v. Lozen Int’l*, 285 F.3d 808 (9th Cir.2002) (ruling that trial court properly considered electronically generated bill of lading as an exhibit to a summary judgment motion. The only foundation that was required was that the record was produced from the same electronic information that was generated contemporaneously when the parties entered into their contact. The court did not require evidence that the records were reliable or accurate).

In contrast, in the case of *In re Vee Vinhnee*, the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. 336 B.R. 437. The court noted that “it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground.” *Id.* at 445-46. The court further observed that:

“The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the *558 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

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

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.”

Id. at 444. The court reasoned that, for paperless electronic records:

“The 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 445. In order to meet the heightened demands for authenticating electronic business records, the court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried:^{FN36}

FN36. IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.03[2].

Professor Imwinkelried perceives electronic records as a form of scientific evidence and discerns an eleven-step foundation for computer records:

- “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 the position taken by the court in *In re Vee Vinhnee* appears to be the most demanding requirement for authenticating computer stored records, other courts also have recognized a need to demonstrate the accuracy of these records. See, e.g., *State v. Dunn*, 7 S.W.3d 427, 432 (Mo.Ct.App.2000) (Admissibility of computer-generated records “should be determined on the basis of the reliability and accuracy of the process involved.”); *State v. Hall*, 976 S.W.2d 121, 147 (Tenn.1998) (“[T]he admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.”)^{FN37}.

FN37. In addition to their insight regarding the authentication of electronic records, these cases are also important in connection to the analysis of whether certain types of electronically stored records constitute hearsay when offered for their substantive truth.

As the foregoing cases illustrate, there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed. Further, it would not be surprising to find that, to date, more courts have tended towards the lenient rather than the demanding approach. However, it also is plain that commentators and courts increasingly recognize the special characteristics of electronically stored records, and there appears to be a growing awareness, as expressed in the *Manual for Complex Litigation*,^{FN38} that courts “should ... con-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

sider the accuracy and reliability of computerized evidence” in ruling on *559 its admissibility. Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Further, although “it may be better to be lucky than good,” as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.

FN38. MANUAL FOR COMPLEX LITIGATION at § 11.446.

The methods of authentication most likely to be appropriate for computerized records are 901(b)(1) (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).

Computer Animation and Computer Simulations.

Two similar, although distinct, forms of computer generated evidence also raise unique authentication issues. The first is computer animation, “the display of a sequence of computer-generated images.” IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a]. The attraction of this form of evidence is irresistible, because:

“when there is no movie or video of the event being litigated, a computer animation is a superior method of communicating the relevant information to the trier of fact. Absent a movie or video, the proponent might have to rely on static charts or oral testimony to convey a large amount of complex information to the trier of fact. When the proponent relies solely on oral expert testimony, the details may be presented one at a time; but an animation can piece all the details together for the jury. A computer animation in effect condenses the information into a single evidentiary package. In part due to television, the typical American is a primarily visual learner; and for that reason, in the short term, many jurors find the animation more understandable than charts or oral testimony. Use of an animation can also significantly increase long-term juror retention of the

information.”

Id. at § 4.09[4][a]. The second form of computer generated evidence is a computer simulation. The distinction between them has been explained usefully 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's 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.”

Thus, the classification of a computer-generated exhibit as a simulation or an animation also affects the evidentiary foundation required for its admission.

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

Courts generally have 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 to illustrate the testimony given in the case. This usually is the sponsoring witness. *Id.* at 10 (state's expert witness had knowledge of content of shaken infant syndrome animation and could testify that it correctly and adequately portrayed the facts that would illustrate her testimony); Hinkle v. City of Clarksburg, 81 F.3d 416 (4th Cir.1996) (holding that a computer-animated videotaped recreation of events at issue in trial is not unduly prejudicial if it is sufficiently close to the actual events and is not confused by the jury for the real life events themselves); Friend v. Time Mfg. Co., 2006 WL 2135807, at *7 (D.Ariz. July 28, 2006) (“The use of computer animations is allowed when it satisfies the usual foundational requirements for demonstrative evidence. ‘At a minimum, the animation's proponent must show the computer simulation fairly and accurately depicts *560 what it represents, whether through the computer expert who prepared it or some other witness who is qualified to so testify, and the opposing party must be afforded an opportunity for

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

cross-examination.’ ” (citation omitted)); *People v. Cauley*, 32 P.3d 602 (Colo.App.2001) (holding that, “[a] computer animation is admissible as demonstrative evidence if the proponent of the video proves that it: 1) is authentic ...; 2) is relevant ...; 3) is a fair and accurate representation of the evidence to which it relates; and 4) has a probative value that is not substantially outweighed by the danger of unfair prejudice ...”); *Clark v. Cantrell*, 339 S.C. 369, 529 S.E.2d 528 (2000) (“[A] party may authenticate a video animation by offering testimony from a witness familiar with the preparation of the animation and the data on which it is based ... [including] the testimony of the expert who prepared the underlying data and the computer technician who used that data to create it.” (citation omitted)). Thus, the most frequent methods of authenticating computer animations are 901(b)(1) (witness with personal knowledge), and 901(b)(3) (testimony of an expert witness).

Computer simulations are treated as a form of scientific evidence, offered for a substantive, rather than demonstrative purpose. WEINSTEIN at § 900,03[1] (p. 900-21); IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a], [c]. The case most often cited with regard to the foundational requirements needed to authenticate a computer simulation is *Commercial Union v. Boston Edison*, where the court stated:

“The function of computer programs like TRACE ‘is to perform rapidly and accurately an extensive series of computations not readily accomplished without use of a computer.’ We permit experts to base their testimony on calculations performed by hand. There is no reason to prevent them from performing the same calculations, with far greater rapidity and accuracy, on a computer. Therefore ... we treat computer-generated models or simulations like other scientific tests, and condition admissibility on a sufficient showing 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.”

412 Mass. 545, 591 N.E.2d 165, 168 (1992) (citation omitted). The *Commercial Union* test has been followed by numerous courts in determining the

foundation needed to authenticate computer simulations. For example, in *State v. Swinton*, the court cited with approval *Commercial Union*, but added that the key to authenticating computer simulations is to determine their reliability. 268 Conn. 781, 847 A.2d 921, 942 (2004). In that regard, the court noted that the following problems could arise with this type of computer evidence: (1) the underlying information itself could be unreliable; (2) the entry of the information into 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 and retrieving it later” could be unreliable; (6) the output of the computer—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. The court noted that Rule 901(b)(9) was a helpful starting point to address authentication of computer simulations. *Id.*; see also *Bray v. Bi-State Dev. Corp.*, 949 S.W.2d 93 (Mo.Ct.App.1997) (citing *Commercial Union* and ruling that authentication properly was accomplished by a witness with knowledge of how the computer program worked, its software, the data used in the calculations, and who verified the accuracy of the calculations made by the computer with manual calculations); *Kudlacek v. Fiat*, 244 Neb. 822, 509 N.W.2d 603, (1994) (citing *Commercial Union* and holding that computer simulation was authenticated by the plaintiff’s expert witness). Thus, the most frequent methods of authenticating computer simulations are 901(b)(1) (witness with personal knowledge); and 901(b)(3) (expert witness). Use of an expert witness to authenticate a computer simulation likely will also *561 involve Federal Rules of Evidence 702 and 703.

Digital Photographs

Photographs have been authenticated for decades under Rule 901(b)(1) by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately represents the scene. Calling the photographer or offering expert testimony about how a camera works almost never has been required for traditional film photographs. Today, however, the vast majority of photographs taken, and offered as exhibits at trial, are digital photographs, which are not made from film, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered. Indeed, unlike photographs made from film, digital photographs may be “enhanced.” Digital image “enhancement consists of removing, inserting, or highlighting an aspect of the photograph that the technician wants to change.” Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005, at 48. Some examples graphically illustrate the authentication issues associated with digital enhancement of photographs:

“[S]uppose that in a civil case, a shadow on a 35 mm photograph obscures the name of the manufacturer of an offending product. The plaintiff might offer an enhanced image, magically stripping the shadow to reveal the defendant’s name. Or suppose that a critical issue is the visibility of a highway hazard. A civil defendant might offer an enhanced image of the stretch of highway to persuade the jury that the plaintiff should have perceived the danger ahead before reaching it. In many criminal trials, the prosecutor offers an ‘improved’, digitally enhanced image of fingerprints discovered at the crime scene. The digital image reveals incriminating points of similarity that the jury otherwise would never would have seen.”

Id. at 49. There are three distinct types of digital photographs that should be considered with respect to authentication analysis: original digital images, digitally converted images, and digitally enhanced images. *Id.*

An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it. *Id.* If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under Rule 201. *Id.* For digitally converted images, authentication requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images, Rules 901(b)(1) and 901(b)(9)—the later rule implicating expert testimony under Rule 702. *Id.* Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo produced from

the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion. *Id.*

For digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified. In such a case, there will need to be proof, permissible under Rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under Rule 702. *Id.* Recently, one state court has given particular scrutiny to how this should be done. In *State v. Swinton*, the defendant was convicted of murder in part based on evidence of computer enhanced images prepared using the Adobe Photoshop software. 268 Conn. 781, 847 A.2d 921, 950-52 (2004). The images showed a superimposition of the defendant’s teeth over digital photographs of bite marks taken from the victim’s body. At trial, the state called the forensic odontologist (bite mark expert) to testify that the defendant was the source of the bite marks on the victim. However, the defendant testified that he was not familiar with how the Adobe Photoshop made the overlay photographs, which involved*562 a multi-step process in which a wax mold of the defendant’s teeth was digitally photographed and scanned into the computer to then be superimposed on the photo of the victim. The trial court admitted the exhibits over objection, but the state appellate court reversed, finding that the defendant had not been afforded a chance to challenge the scientific or technical process by which the exhibits had been prepared. The court stated that to authenticate the exhibits would require a sponsoring witness who could testify, adequately and truthfully, as to exactly what the jury was looking at, and the defendant had a right to cross-examine the witness concerning the evidence. Because the witness called by the state to authenticate the exhibits lacked the computer expertise to do so, the defendant was deprived of the right to cross examine him. *Id.* at 950-51.

Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a means to authenticate digitally enhanced photographs under Rule 901(b)(9): (1) The witness is an expert in digital photography; (2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

process by which the computer manipulates them; (3) the witness testifies that the processes used are valid; (4) the witness testifies that there has been “adequate research into the specific application of image enhancement technology involved in the case”; (5) the witness testifies that the software used was developed from the research; (6) the witness received a film photograph; (7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer; (8) the witness can identify the trial exhibit as the product of the enhancement process he or she performed. Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005 at 54. The author recognized that this is an “extensive foundation,” and whether it will be adopted by courts in the future remains to be seen. *Id.* However, it is probable that courts will require authentication of digitally enhanced photographs by adequate testimony that it is the product of a system or process that produces accurate and reliable results. FED.R.EVID. 901(b)(9).

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced. Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in Rules 901 and 902, as well as consider requesting a stipulation from opposing counsel, or filing a request for admission of the genuineness of the evidence under Rule 36 of the Federal Rules of Civil Procedure. With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

In this case, neither plaintiffs nor defendants provided any authenticating facts for the e-mail and other evidence that they proffered in support of their summary judgment memoranda—they simply attached the exhibits. This complete absence of authentication stripped the exhibits of any evidentiary value because the Court could not consider them as evidentiary facts. This, in turn, required the dismissal, without prejudice, of the cross motions for summary judgment, with

leave to resubmit them once the evidentiary deficiencies had been cured.

Hearsay (Rules 801-807)

The fourth “hurdle” that must be overcome when introducing electronic evidence is the potential application of the hearsay rule. Hearsay issues are pervasive when electronically stored and generated evidence is introduced. To properly analyze hearsay issues there are five separate questions that must be answered: (1) does the evidence constitute a **statement**, as defined by Rule 801(a); (2) was the statement made by a “**declarant**,” as defined by Rule 801(b); (3) is the statement being offered to prove the **truth of its contents**, as provided by Rule 801(c); *563 (4) is the statement **excluded from the definition of hearsay by rule 801(d)**; and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807. It is critical to proper hearsay analysis to consider each of these questions.

The requirements of a “Statement,” Rule 801(a), made by a “Person”, Rule 801(b)

Rule 801(a) states:

“A ‘statement’ is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion.”

The key to understanding the hearsay rule is to appreciate that it only applies to intentionally assertive verbal or non-verbal conduct, and its goal is to guard against the risks associated with testimonial evidence: perception, memory, sincerity and narration. FED.R.EVID. 801 advisory committee's note (“The factors to be considered in evaluating the testimony of a witness are perception, memory, and narration. Sometimes a fourth is added, sincerity.”) (citations omitted); WEINSTEIN at § 801. 11[1] (“To be considered hearsay, a statement out of court must be offered in evidence to prove the truth of the matter it asserts. This part of the definition arises out of the factfinder's need to assess the credibility of the person who made a statement offered for its truth. When a witness testifies in court, the trier can assess the witness's perception, narration and memory to determine whether the testimony accurately represents the facts observed.”); PAUL R. RICE, *ELECTRONIC EVIDENCE: LAW AND PRACTICE*, 262 (ABA Publishing 2005)(hereinafter “RICE”) (“Hearsay is an

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination.”).

The use of the word “statement” in Rule 801(a) is a critical component of the hearsay rule. WEINSTEIN at § 801.10[1] (“Because Rule 801 describes hearsay as an out-of-court *statement* offered as proof as [sic] the matter asserted, the definition of ‘statement’ is of critical importance.”); SALTZBURG at § 801.02[1][c] (“If proffered evidence is not a ‘statement’ within the meaning of Rule 801(a), then it cannot be hearsay, and so cannot be excluded under the [hearsay] Rule.”). The word is used in a very precise, and non-colloquial sense—it only applies to verbal conduct (spoken or written) or non-verbal conduct that is intended by a human declarant to be *assertive*. The advisory committee note to Rule 801(a) states this concept squarely:

“The definition of ‘statement’ assumes importance because the term is used in the definition of hearsay in subdivision (c). The effect of the definition of ‘statement’ is to exclude from the operation of the hearsay rule all evidence of conduct, verbal or nonverbal, not intended as an assertion. The key to the definition is that nothing is an assertion unless intended to be one.”

Ironically, the word “assertion” is not defined in the hearsay rule, despite its importance to the concept. An assertion usefully may be defined as “to state as true; declare; maintain.” Black’s Law Dictionary 106 (5th ed.1979).

Although there is not universal agreement on this point, it appears that for verbal or nonverbal conduct to fall within the definition of the hearsay rule as defined under the federal rules of evidence, it must be either an expressly assertive written or spoken utterance, or nonverbal conduct expressly intended to be an assertion—the federal rules appear to have excluded from the definition of hearsay “implied assertions”—or unstated assertions that are inferred from verbal or nonverbal conduct. The advisory committee’s note to

Rule 801(a) supports the notion non-verbal conduct that is not assertive, and verbal conduct (spoken or written) ^{FN39} that is non-assertive should be viewed the same *564 way—falling outside the definition of a “statement:”

FN39. An example of nonassertive written verbal conduct would be to write a person’s name and address on an envelope. An example of nonassertive spoken verbal conduct would be to ask a question that does not contain within it a factual assertion “Is it going to rain tomorrow?”

“[N]onverbal conduct ... may be offered as evidence that the person acted as he did because of his belief in the existence of the condition sought to be proved, from which belief the existence of the condition may be inferred. This sequence is, arguably, in effect an assertion of the existence of the condition and hence properly includable within the hearsay concept. Admittedly, evidence of this character is untested with respect to the perception, memory, and narration (or their equivalents) of the actor, but the Advisory Committee is of the view that these dangers are minimal in the absence of an intent to assert and do not justify the loss of the evidence on hearsay grounds. No class of evidence is free of the possibility of fabrication, but the likelihood is less with nonverbal than with assertive verbal conduct. The situations giving rise to the nonverbal conduct are such as virtually to eliminate questions of sincerity.... *Similar considerations govern nonassertive verbal conduct and verbal conduct which is assertive but offered as a basis for inferring something other than the matter asserted, also excluded from the definition of hearsay by the language of subdivision (c).*”

FED.R.EVID. 801(a) advisory committee’s note (emphasis added) (citation omitted); Wilson v. Clancy, 747 F.Supp. 1154, 1158 (D.Md.1990) (“It appears to be the intent of the limitation of the hearsay definition under FED.R.EVID. 801(a)(2) to non-verbal conduct ‘intended by the [declarant] as an assertion’ to do away with the notion that ‘implied assertions’ are within the hearsay prohibition.” (alterations in original) (citation omitted)); WEINSTEIN at § 801.10[2][c]; ^{FN40} SALTZBURG at § 801.02[1][c]. ^{FN41}

FN40. “Words and actions may convey

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

meaning even though they were not consciously intended as assertions. Sometimes the relevance of words or actions to show a particular fact depends on drawing an inference that a person would not have spoken or acted in a certain way unless the person believed a relevant fact to be true. According to the Advisory Committee, the 'key to the definition is that nothing is an assertion unless it is intended to be'. Many courts have found that words or conduct offered to show the actor's implicit beliefs do not constitute statements under the hearsay rule unless they were intended by the actor as an assertion.... Other courts, however, have noted that an oral or written declaration is hearsay if offered to show the truth of a matter implied by its contents."

FN41. "Common-law jurisdictions divide on whether nonverbal conduct that is not intended as an assertion is hearsay if it is introduced to show the truth of the actor's underlying beliefs.... The reasons for excluding non-assertive conduct from the hearsay rule are persuasive. A principal reason for excluding hearsay is that the veracity of the declarant cannot be tested by cross-examination. In the case of non-assertive acts, the actor by definition does not intend to make an assertion, meaning that the risk of insincerity is substantially diminished. The actor is at least not trying to lie. Moreover, non-assertive conduct is usually more reliable than the ordinary out-of-court statement, because by conduct the declarant has risked action on the correctness of his belief-he has put his money where his mouth is."

The second question that must be answered in the hearsay analysis is closely tied to the first. A writing or spoken utterance cannot be a "statement" under the hearsay rule unless it is made by a "declarant," as required by Rule 801(b), which provides "[a] 'declarant' is a *person* who makes a statement." (emphasis added). When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received,

there is no "person" involved in the creation of the record, and no "assertion" being made. For that reason, the record is not a statement and cannot be hearsay.

Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements" under Rule 801(a). Where the writings are non-assertive, or not made by a "person," courts have held that they do not constitute hearsay, as they are not "statements." United States v. Khorozian, 333 F.3d 498, 506 (3d Cir.2003) ("[N]either the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by "a person," so nothing "said" by a machine ... is hearsay' " (second alteration in original)); *565 Safavian, 435 F.Supp.2d at 44 (holding that portions of e-mail communications that make imperative statements instructing defendant what to do, or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay); Telewizja Polska USA, 2004 WL 2367740 (finding that images and text posted on website offered to show what the website looked like on a particular day were not "statements" and therefore fell outside the reach of the hearsay rule); Perfect 10, 213 F.Supp.2d at 1155 (finding that images and text taken from website of defendant not hearsay, "to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all-and thus fall outside the ambit of the hearsay rule."); United States v. Rollins, rev'd on other grounds 2004 WL 26780, at *9 (A.F.Ct.Crim.App. Dec.24, 2003) ("Computer generated records are not hearsay: the role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system itself, relative to its proper functioning and accuracy."); State v. Dunn, 7 S.W.3d 427, 432 (Mo.Ct.App.2000) ("Because records of this type [computer generated telephone records] are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the reliability and accuracy of the process involved."); State v. Hall, 976 S.W.2d 121, 147 (Tenn.1998) (reviewing the admissibility of computer generated rec-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

ords and holding “[t]he role that the hearsay rule plays in limiting the fact finder’s consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.”).

The requirement that the statement be offered to prove its substantive truth.

The third question that must be answered in determining if evidence is hearsay is whether the statement is offered to prove its substantive truth, or for some other purpose. Rule 801(c) states: “Hearsay is 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.*” (emphasis added). Thus, even if the evidence is an assertion, made by a declarant, it still is not hearsay unless offered to prove the truth of what is asserted. The advisory committee’s note to Rule 801(c) underscores this: “If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay. The effect is to exclude from hearsay the entire category of ‘verbal acts’ and ‘verbal parts of an act,’ in which the statement itself affects the legal rights of the parties or is a circumstance bearing on conduct affecting their rights.” FED.R.EVID. 801(c) advisory committee’s note (citation omitted). *See also* WEINSTEIN at § 801.11[1] (“‘If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted.’ Thus, if a declarant’s statement is not offered for its truth, the declarant’s credibility is not material, and the statement is not hearsay.” (citation omitted)). Commentators have identified many instances in which assertive statements are not hearsay because they are not offered to prove the truth of the assertions: (1) statements offered to prove a claim that the statement was false or misleading, as in a fraud or misrepresentation case; ^{FN42} (2) statements offered to “prove that because they were made, listeners had notice or knowledge of the information related in the statements,” or to show the effect on the listener of the statement; ^{FN43} (3) statements “offered to prove an association*566 between two or more persons;” ^{FN44} (4) statements offered as circumstantial evidence of the declarant’s state of mind, ^{FN45} or motive; ^{FN46} (5) statements that have relevance simply because they

were made, regardless of their literal truth or falsity—the so called “verbal acts or parts of acts,” ^{FN47} also referred to as “legally operative facts”; ^{FN48} and (6) statements that are questions or imperative commands, ^{FN49} such as “what time is it” or “close the door.”

FN42. SALTZBURG at § 801.02[1][e].

FN43. *Id.* at § 801.02[1][f]; WEINSTEIN at § 801.11[5][a].

FN44. SALTZBURG at § 801.2[1][g]; *see also* WEINSTEIN at § 801.11[6].

FN45. SALTZBURG at § 801.02[1][h]. This category typically deals with statements from which the declarant’s state of mind is circumstantially inferred. For example, if someone says “Woe is me” it may be inferred that they are depressed or sad. Such statements are in contrast to statements that constitute direct evidence of the declarant’s state of mind, offered to prove that state of mind, for example “I feel good,” offered to prove that the declarant felt good. The later example is hearsay, but covered by an exception, Rule 803(3): Then existing state of mind or condition.

FN46. WEINSTEIN at § 801.11[5][a], [c].

FN47. SALTZBURG at § 801.02[1][j].

FN48. WEINSTEIN at § 801.11[3]-[4].

FN49. *Id.* at § 801.11[2].

When analyzing the admissibility of electronically generated evidence, courts also have held that statements contained within such evidence fall outside the hearsay definition if offered for a purpose other than their substantive truth. Siddiqui, 235 F.3d at 1323 (e-mail between defendant and co-worker not hearsay because not offered to prove truth of substantive content, but instead to show that a relationship existed between defendant and co-worker, and that it was customary for them to communicate by e-mail); Safavian, 435 F.Supp.2d at 44 (e-mail from lobbyist to defendant not hearsay because they were not offered

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

to prove their truth, but to illustrate the nature of the lobbyist's work on behalf of clients to provide context for other admissible e-mail; and as evidence of the defendant's intent, motive and state of mind); *Telewizja Polska USA*, 2004 WL 2367740; *Perfect 10*, 213 F.Supp.2d at 1155 (exhibits of defendant's website on a particular date were not "statements" for purposes of hearsay rule because they were offered to show trademark and copyright infringement, therefore they were relevant for a purpose other than their literal truth); *State v. Braidic*, 119 Wash.App. 1075, 2004 WL 52412 at *1 (Jan. 13, 2004) (e-mail sent by defendant to victim not hearsay because they were not offered to prove the truth of the statements.).

Finally, of particular relevance to this suit are the cases that have held that communications between the parties to a contract that define the terms of a contract, or prove its content, are not hearsay, as they are verbal acts or legally operative facts. See, e.g., *Preferred Properties Inc. v. Indian River Estates Inc.*, 276 F.3d 790, 799 n. 5 (6th Cir.2002) (verbal acts creating a contract are not hearsay); *Kepner-Tregoe, Inc. v. Leadership Software*, 12 F.3d 527, 540 (5th Cir.1994) (finding contract to be a signed writing of independent legal significance and therefore non-hearsay); *Mueller v. Abdnor*, 972 F.2d 931, 937 (8th Cir.1992) (holding contracts and letters from attorney relating to the formation thereof are non-hearsay); *United States v. Tann*, 425 F.Supp.2d 26, 29 (D.D.C.2006) (finding negotiable instruments to be legally operative documents that do not constitute hearsay); *Planmatics*, 137 F.Supp.2d at 621 (D.Md.2001) (holding testimony regarding instructions made to individuals is not hearsay because instructions were not statements of fact). See also WEINSTEIN at § 801.11[3].^{FN50} Because the e-mails that the parties to this suit attached as unauthenticated exhibits to their summary judgment papers were introduced for the purpose of proving the making of the agreement to arbitrate the dispute regarding the damage caused by the lightning strike, and the terms of this agreement, *567 they are not hearsay if offered for this purpose because they are verbal acts, or legally operative facts. What the parties did not do, however, was articulate the non-hearsay purpose for which the e-mails were offered; they merely attached them as exhibits, without further explanation of the purpose for which they were offered, or clarification that they were not offered for their substantive truth. Because evidence may be offered for more than one purpose, it may be relevant for its substantive truth, and potentially hearsay, or rele-

vant for some other purpose, and non-hearsay. For this reason it is important for a party offering an exhibit into evidence to clearly explain each purpose for which it is offered, and address any hearsay issues associated with each purpose for which it is offered.

FN50. A verbal act is an utterance of an operative fact that gives rise to legal consequences. Verbal acts, also known as statements of legal consequence, are not hearsay, because the statement is admitted merely to show that it was actually made, not to prove the truth of what was asserted in it. For example, the hearsay rule does not exclude relevant evidence as to what the contracting parties said or wrote with respect to the making or the terms of an agreement.

Is the evidence excluded from the definition of hearsay by Rule 801(d)(1) or 801(d)(2).

Once it has been determined whether evidence falls into the definition of hearsay because it is a statement, uttered by a declarant, and offered for its substantive truth, the final step in assessing whether it is hearsay is to see if it is excluded from the definition of hearsay by two rules: 801(d)(1), which identifies three types of prior statements by witnesses who actually testify and are subject to cross examination, which are excluded from the definition of hearsay, and 801(d)(2), which identifies five types of admissions by a party opponent that are excluded from the definition of hearsay. FED.R.EVID. 801(d) advisory committee's note ("[s]everal types of statements which would otherwise literally fall within the definition [of hearsay] are expressly excluded from it ..."); WEINSTEIN at § 801[20][1] & 801[30][1]; SALTZBURG at § 801.02[2] & 801.02[6].

Rule 801(d)(1) identifies three types of prior witness statements that are excluded from the definition of hearsay: first, 801(d)(1)(A) excludes prior inconsistent "testimonial statements" made under oath at a trial, hearing, court proceeding or deposition; next, 801(d)(1)(B) excludes prior consistent statements offered to rebut an express or implied allegation of recent fabrication, or improper influence or motive; and finally, 801(d)(1)(C) excludes statements of identification of a person made after perceiving that person. For each of these exceptions, it is required that the declarant testify at trial and be subject to cross examination about the prior statements. FED. R.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

EVID 801(d)(1); FED.R.EVID. 801(d)(1) advisory committee's note (“[Rule 801(d)(1)] requires in each instance, as a general safeguard, that the declarant actually testify as a witness, and it then enumerates three situations in which the statement is excepted from the category of hearsay.”); WEINSTEIN at § 801.20[2] (“For a prior witness statement to escape the hearsay rule, the declarant must testify at trial and be subject to cross-examination concerning the statement.” (citation omitted)).

Rule 801(d)(2) identifies five types of statements as “admissions by a party opponent,” and excludes them from the definition of hearsay. Specifically: 801(d)(2)(A) excludes the party's own statement, made in either an individual or representative capacity; 801(d)(2)(B) addresses a statement by another that a party has adopted or manifested a belief in its truth; 801(d)(2)(C) deals with a statement by a person authorized by a party to make a statement concerning a subject; 801(d)(2)(D) excludes a statement made by a party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the agency or employment relationship; and 801(d)(2)(E) excludes the statement of a co-conspirator of a party made during the existence of the conspiracy and in furtherance of the conspiracy. To qualify as an admission, the party's out-of-court statement must be offered against that party, it cannot offer its own out of court statements as admissions. WEINSTEIN at § 801.30[1] (“To be admissible under [Rule 801(d)(2)], the party's statements must be offered *against* that party. A party cannot use this provision to offer his or her own statements into evidence.”).

As can be seen from reading Rule 801(d)(1) and (2), there are specific foundational facts that must be established before the statement or admission can be accepted into evidence. These determinations are made by the trial judge under Rule 104(a), and therefore the rules of evidence, except *568 for privilege, are inapplicable. FED.R.EVID. 104(a), 1101(d)(1); FED.R.EVID. 104(a) advisory committee's note (“[W]hen a hearsay statement is offered as a declaration against interest, a decision must be made whether it possesses the required against-interest characteristics. These decisions too, are made by the judge.”)

Given the near universal use of electronic means

of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party. Siddiqui, 235 F.3d at 1323 (ruling that e-mail authored by defendant was not hearsay because it was an admission under Rule 801(d)(2)(A)); Safavian, 435 F.Supp.2d at 43-44 (holding that e-mail sent by defendant himself was admissible as non-hearsay because it constituted an admission by the defendant, 801(d)(2)(A), and as an “adoptive admission” under Rule 801(d)(2)(B)); Telewizja Polska USA, 2004 WL 2367740 (N.D.Ill. Oct.15, 2004) (holding exhibits showing defendant's website as it appeared on a certain day were admissible as admissions against defendant); Perfect 10, 213 F.Supp.2d at 1155 (admitting e-mail sent by employees of defendant against the defendant as admissions under 801(d)(2)(D)).

If, after applying the foregoing four-step analysis, it is determined that the electronic evidence constitutes a statement by a person that is offered for its substantive truth and is not excluded from the definition of hearsay by Rule 801(d)(1) or (2), then the evidence is hearsay, and is inadmissible unless it qualifies as one of many hearsay exceptions identified by Rule 803, 804 and 807. The process of determining whether hearsay falls into one of the many exceptions can appear daunting, because there are twenty-three identified in Rule 803, five in Rule 804, and Rule 807, the so-called “catch-all” exception, allows exceptions to be tailor made. Upon closer examination, however, the task is less onerous because the number of hearsay exceptions can be categorized in helpful ways that make them more manageable, and in most instances a handful of hearsay exceptions repeatedly are used in connection with electronically generated or stored evidence. Familiarity with these rules will suffice in most instances to overcome hearsay objections routinely made to ESI.

Rule 803 contains twenty-three separate hearsay exceptions. At first glance they may seem like they have nothing in common, but they do. All twenty-three are admissible regardless of whether the declarant is available to testify, distinguishing them from the five exceptions in Rule 804, each of which is inapplicable unless the declarant is “unavailable,” as defined by any of the five methods identified in Rule 804(a). In addition, the twenty-three exceptions in Rule 803 may be grouped in three broad categories:

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

Category 1 includes exceptions dealing with **perceptions, observations, state of mind, intent and sensation** 803(1) (present sense impressions); 803(2) (excited utterances); 803(3) (then existing state of mind, condition or sensation); 803(4) (statements in furtherance of medical diagnosis and treatment). **Category 2** includes **documents, records, and other writings** 803(5) (past recollection recorded); 803(6) & (7) (business records); 803(8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12) (certificates of baptism, marriage and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) (ancient documents); 803(18) (learned treatises); 803(22) (judgments of conviction in a criminal case); and 803(23) (judgments in certain kinds of civil cases). **Category 3** includes statements dealing with **reputation** 803(19) (reputation regarding personal or family history); 803(20) (reputation regarding custom, use and practice associated with land, and historically significant facts); and 803(21) (reputation regarding character within the community and among associates).

Given the widely accepted fact that most writings today are created and stored in electronic format, it is easy to see that the many types of documents and writings covered in Rule 803 will implicate electronic writings. Similarly, given the ubiquity of communications in electronic media (e-mail, *569 text messages, chat rooms, internet postings on servers like “myspace” or “youtube” or on blogs, voice mail, etc.), it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium. It would unnecessarily prolong an already lengthy opinion to analyze all of the implications of the hearsay exceptions in Rule 803 as they relate to ESI. It is possible, however, to focus on the handful that have been discussed by the courts and that are most likely to be used in a hearsay analysis of ESI. Because the court's research has shown that the Rule 803 hearsay exceptions, rather than those found in Rules 804 or 807, have been cited by courts evaluating the hearsay implications of electronic evidence, the following analysis will be confined to that rule.

Rule 803(1) Present Sense Impression

Rule 803(1) creates an exception from exclusion under the hearsay rule for:

“(1) Present sense impression. A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.”

There are three elements that must be met for this hearsay exception to apply: (1) the declarant must have personally perceived the event that is described in the statement; (2) the statement must be a simple explanation or description of the event perceived; and (3) the declaration and the event described must be contemporaneous. WEINSTEIN at § 803.03[1]. Present sense impressions are considered trustworthy because the near simultaneous expression of the explanation or description of the event with its perception militates against any memory deficiency, or opportunity to intentionally misstate what occurred. FED.R.EVID. 803(1) advisory committee's note (“The underlying theory of Exception (1) is that substantial contemporaneity of event and statement negate the likelihood of deliberate or conscious misrepresentation.”); WEINSTEIN at § 803.03[1].

Rule 803(2) Excited Utterance

Closely related to Rule 803(1) is Rule 803(2),^{FN51} the excited utterance exception to the hearsay rule, which provides:

^{FN51}. See FED.R.EVID. 803(1)-(2) advisory committee's note (“Exceptions (1) and (2) [to Rule 803]. In considerable measure these two examples overlap, though based on somewhat different theories. The most significant practical difference will lie in the time lapse allowable between the event and statement.”).

“(2) Excited utterance. A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.”

The theory behind the excited utterance exception is that perception of a startling or exciting event produces in the declarant an emotional state that reduces the likelihood that the description of the event while under this emotional state will be inaccurate or purposely misstated. FED.R.EVID. 803(2) ad-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

visory committee's note ("The theory of Exception (2) is simply that circumstances may produce a condition of excitement which temporarily stills the capacity of reflection and produces utterances free of conscious fabrication."); WEINSTEIN at § 803.04[1] ("The premise underlying the exception for excited utterances is that a person under the influence of excitement precipitated by an external startling event will not have the reflective capacity essential for fabrication.").

The prevalence of electronic communication devices, and the fact that many are portable and small, means that people always seem to have their laptops, PDA's, and cell phones with them, and available for use to send e-mails or text messages describing events as they are happening. Further, it is a common experience these days to talk to someone on the phone and hear them typing notes of the conversation on a computer as you are talking to them. For these reasons, Rules 803(1) and (2) may provide hearsay exceptions for electronically stored communications containing either present sense impressions or excited utterances. See, e.g., *United States v. Ferber*, 966 F.Supp. 90 (D.Mass.1997) (holding that e-mail from employee to boss about substance of telephone call with defendant in mail/wire fraud case *570 did qualify as a present sense expression under Rule 803(1), but did not qualify as an excited utterance under Rule 803(2), despite the language at the end of the e-mail "my mind is mush."); *State of New York v. Microsoft*, 2002 WL 649951 (D.D.C. Apr.12, 2002) (analyzing the admissibility of series of exhibits including e-mail and e-mail "chains" under various hearsay exceptions, and ruling that an e-mail prepared several days after a telephone call that described the call did not qualify as a present sense impression under Rule 803(1) because the requirement of "contemporaneity" was not met).

Rule 803(3) Then Existing State of Mind or Condition

Rule 803(3) provides a hearsay exception for:

"(3) Then existing mental, emotional, or physical condition. A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the

execution, revocation, identification, or terms of declarant's will."

Rule 803(3) also is closely related to Rule 803(1). See FED.R.EVID. 803(3) advisory committee's note ("Exception (3) [to Rule 803] is essentially a specialized application of Exception (1), presented separately to enhance its usefulness and accessibility."). The rule permits the statement of the declarant's state of mind, sensation, mental, emotional, or physical condition, as well as statements of motive, intent, plan or design, but excludes statements of memory or belief if offered to prove the truth of the fact remembered. FED.R.EVID. 803(3) advisory committee's note ("The exclusion of 'statements of memory or belief to prove the fact remembered or believed' is necessary to avoid the virtual destruction of the hearsay rule which would otherwise result from allowing state of mind, provable by a hearsay statement, to serve as the basis for an inference of the happening of the event which produced the state of mind."). The foundation for proving an exception under Rule 803(3) is: (1) The statement must be contemporaneous with the mental state being proven; (2) There must be [an absence of] suspicious circumstances that would evidence a motive for fabrication or misrepresentation of the declarant's state of mind; and (3) The state of mind of the declarant must be relevant in the case. WEINSTEIN at § 803.05[2][a]. Rule 803(3) has been used to prove a wide variety of matters, including the reason why the declarant would not deal with a supplier or dealer, motive, competency, ill-will, motive, lack of intent to defraud, willingness to engage in criminal conduct, the victim's state of mind in an extortion case, and confusion or secondary meaning in a trademark infringement case. *Id.*

Rule 803(3) is particularly useful when trying to admit e-mail, a medium of communication that seems particularly prone to candid, perhaps too-candid, statements of the declarant's state of mind, feelings, emotions, and motives. Indeed, courts have analyzed this rule in connection with ruling on the admissibility of electronic evidence. In *New York v. Microsoft*, the court analyzed admissibility of e-mail and e-mail chains under a variety of hearsay rules, including 803(3). 2002 WL 649951. It concluded that an e-mail made several days following a telephone conversation did not qualify under Rule 803(3) because it contained more than just the declarant's state of mind, but also included the maker's memory of belief about the

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

events that affected his state of mind, which is specifically excluded by Rule 803(3). *Id.* at *5. See also *Safavian*, 435 F.Supp.2d at 44 (admitting e-mail that contained statements of defendant's state of mind under Rule 803(3)).

Rule 803(6) Business Records

Rule 803(6) recognizes an exception to the hearsay rule for:

“(6) Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business *571 activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term ‘business’ as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.”

The foundational elements for a business record are: (1) The document must have been prepared in the normal course of business; (2) it must have been made at or near the time of the events it records; (3) it must be based on the personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant; ^{FN52} and (4) to have been made in the normal course of business means that the document was made in the regular course of a regularly conducted business activity, for which it was the regular practice of the business to maintain a memorandum. WEINSTEIN at § 803.08[1]. It is essential for the exception to apply that it was made in furtherance of the business' needs, and not for the personal purposes of the person who made it. Given the fact that many employees use the computers where they work for personal as well as business reasons, some care must be taken to analyze whether the business record exception is applicable, especially to e-mail.

FN52. The majority view is that the source of

the information memorialized in the business record must have a business duty to transmit the information to the maker of the record, if the maker him or herself lacks personal knowledge of the facts or events. See, e.g., FED.R.EVID. 803(3) 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 the 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, provided the recipient of the information has a business duty to verify the accuracy of the information provided. See, e.g., *Rambus*, 348 F.Supp.2d at 706-07 (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.” (citation omitted)).

Rule 902(11) also is 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 the following:

“(11) Certified domestic records of regularly con-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

ducted activity. 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.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.”

*572 Because the elements for both rules are essentially identical, they frequently are analyzed together when Rule 902(11) is the proffered means by which a party seek to admit a business record. See *In re Vee Vinhnee*, 336 B.R. at 446; *Rambus*, 348 F.Supp.2d at 701 (holding that analysis of Rule 803(6) and 902(11) go “hand in hand,” and identifying the following requirements for authentication under Rule 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 maintain the record).

The business record exception is one of the hearsay exceptions most discussed by courts when ruling on the admissibility of electronic evidence. The decisions demonstrate a continuum running from cases where the court was very lenient in admitting electronic business records, without demanding analysis, to those in which the court took a very demanding approach and scrupulously analyzed every element of the exception, and excluded evidence when all were not met. For example, in *State of New York v. Microsoft*, the court analyzed the admissibility of “e-mail chains.” 2002 WL 649951 (D.D.C. Apr.12, 2002). The court held that an e-mail prepared by an employee did not qualify as a business record because, while it may have been the regular practice of the employee to send an e-mail following the receipt of a phone call that summarized the call, there had been no showing that it was the regular practice of the employer to require that the employee make and maintain such e-mails. *Id.* at *9. The court was particularly careful in analyzing the hearsay issues associated with e-mail chains involving multiple employees of the same employer. It held that to establish a proper foundation, the proponent would have to show that when the source of the information related in the e-mail is someone other than the maker of the e-mail, that the source, the maker “as well as every other participant in the chain producing the record are, acting in the regular course of [the] business.” *Id.* at *14. If this showing is made, the court ruled, then the multiple levels of hearsay in the e-mail chain are covered by Rule 803(6). However, “[i]f the source of the information is an outsider, Rule 803(6) does not, by itself, permit the admission of the business record. The outsider’s statement must fall within another hearsay exception to be admissible because it does not have the presumption of accuracy that statements made during the regular course of business have.” *Id.* at *14. The court also excluded another e-mail chain for failure of the proponent to establish a proper foundation, saying “[p]laintiffs have not established the requisite foundation that the multiple authors of these e-mails each composed their portion of the document

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

in the course of regularly conducted business activity and that it was the regular practice of RealNetworks to compose such e-mail correspondence. Moreover, the multiple authors and forwarded nature of the e-mails undercuts the reliability of the information contained therein.” *Id.* at *19.

Similarly, in *Rambus Inc. v. Infineon Tech. AG*, the Court critically analyzed the admissibility of e-mail under the business record exception to the hearsay rule. 348 F.Supp.2d 698, 706 (E.D.Va.2004). Certain exhibits objected to by the defendant were e-mail chains prepared at least in part by persons outside of the business entity that maintained the e-mail as part of its records, and which was seeking their admissibility as *573 business records. The court noted that there was “not a requirement that the records have been prepared by the entity that has custody of them, as long as they were created in the regular course of some [other] entity’s business.” *Id.* (quoting WEINSTEIN, at § 803.08[8][a]). The court added “[h]owever, it also is true that: To satisfy Rule 803(6) each participant in the chain which created the record—from the initial observer-reporter to the final entrant—must generally be acting in the course of the regularly conduct[ed] business. *Id.* at 707. If some participant is not so engaged, some other hearsay exception must apply to that link of the chain.” *Id.* at 706.

In contrast to the demanding approach taken in *Rambus* and *New York v. Microsoft*, the court in *United States v. Safavian* took a more flexible approach to the admissibility of e-mail chains. 435 F.Supp.2d 36, 40-41 (D.D.C.2006). The defendant objected to the admissibility of e-mail chains, arguing that they were not trustworthy because they contained e-mails embedded within e-mails. The court overruled this objection, stating:

“[t]he defendant’s argument is more appropriately directed to the weight the jury should give the evidence, not its authenticity. While the defendant is correct that earlier e-mails that are included in a chain—either as ones that have been forwarded or to which another has replied—may be altered, this trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice.... The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a

matter of course.... We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of the nation’s population and is of particular importance in the professional world.... Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done.”

Id. at 41. Notably, the court did not engage in the demanding business records exception analysis that was done by the courts in *Rambus* and *New York v. Microsoft*.

Perhaps the most demanding analysis regarding the admissibility of electronic evidence under the business record exception to the hearsay rule appears in *In re Vee Vinhnee*, 336 B.R. at 445. In this case the appellate bankruptcy panel upheld the trial bankruptcy judge’s exclusion of electronic business records, observing that “early versions of computer foundations [accepted by courts] were too cursory, even though the basic elements [of the business records exception] covered the ground.” The court held that the proponent of an electronic business record was required to show that the paperless electronic record retrieved from its computer files was the same one as originally had been entered into its computer, noting that 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.” *Id.* at 444. It added “[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 questions of whether records have been changed since their creation.” *Id.* at 445. The court reasoned that the “complexity of ever-developing computer technology necessitates more precise focus,” because “digital technology makes it easier to alter text of documents that have been scanned into a database, thereby increasing the im-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

portance of audit procedures designed to assure the continuing integrity of the records.” *Id.*

In contrast to the demanding approach taken in *In re Vee Vinhnee*, many other courts have admitted electronic business records*574 under a much more relaxed standard. See, e.g., *United States v. Kassimu*, 2006 WL 1880335 (5th Cir.2006) (Establishing the foundation for a computer generated business record did not require the maker of the record, or even a custodian, but only a witness qualified to explain the record keeping system of organization.); *United States v. Fujii*, 301 F.3d 535 (7th Cir.2002) (holding that computerized check-in and reservation records were admissible as business records on a showing that the data reflected in the printouts was kept in the ordinary course of the business); *Sea-Land*, 285 F.3d 808 (holding that copy of electronic bill of lading had been properly admitted as a business record because it had been produced from the same electronic information that had been contemporaneously generated when the parties entered into their contract. The court noted that “it is immaterial that the business record is maintained in a computer rather than in company books.” (citation omitted)); *Wapnick v. Commissioner of Internal Revenue*, T.C. Memo.2002-45, 2002 WL 215993 (T.C.2002)(computerized accounting records were admissible as business records because foundation was established by IRS agents who compared the data in the computer records with information in the company’s tax returns, bank statements, and by contacting clients of the company to verify information in the computerized records).

The lesson to be taken from these cases is that some courts will require the proponent of electronic business records or e-mail evidence to make an enhanced showing in addition to meeting each element of the business records exception. These courts are concerned that the information generated for use in litigation may have been altered, changed or manipulated after its initial input, or that the programs and procedures used to create and maintain the records are not reliable or accurate. Others will be content to view electronic business records in the same light as traditional “hard copy” records, and require only a rudimentary foundation. Unless counsel knows what level of scrutiny will be required, it would be prudent to analyze electronic business records that are essential to his or her case by the most demanding standard. The cases further suggest that during pretrial discovery

counsel should determine whether opposing counsel will object to admissibility of critical documents. This can be done by requesting a stipulation, or by proponent requests for admission of fact and genuineness of records under FED.R.CIV.P. 36. If it is known that opposing counsel will object, or refuses to stipulate, or denies a Rule 36 request to admit genuineness, then the lawyer intending to introduce the electronic business record should be prepared to establish the business record exception under the most demanding standard required, to avoid exclusion of the evidence.

Rule 803(8) Public Records.

In addition to the above described hearsay exceptions, courts have found that electronic records also met the requirements of the public records exception under Rule 803(8):

“(8) Public records and reports. Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.”

Furthermore, “[j]ustification for the exception is the assumption that a public official will perform his duty properly, and the unlikelihood that he will remember details independently of the record.” FED.R.EVID. 803(8) advisory committee’s note. Moreover, “[s]ince the assurances of accuracy are generally greater for public records than for regular business records, the proponent is usually not required to establish their admissibility through foundation testimony.... The burden of proof concerning the admissibility of public records is on the party opposing their introduction.” WEINSTEIN at § 803.10[2]. Courts have applied this deferential standard of admissibility for electronic *575 public records. See, e.g., *EEOC v. E.I. DuPont de Nemours and Co.*, 2004 WL 2347556 (holding that table of information compiled by U.S. Census Bureau was admissible as an

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

exception to the hearsay rule as a public record under Rule 803(8), and rejecting claims that the posting of data on the Census Bureau's website rendered it untrustworthy); Lester v. Natsios, 290 F.Supp.2d 11 (D.D.C.2003) (admitting e-mail of public agency, and noting that “[r]ecords of public agencies such as those challenged by plaintiff are generally admissible ... under FED.R.EVID. 803(8).”); United States v. Ocegüerra-Aguirre, 70 Fed.Appx. 473 (9th Cir.2003) (Court held that trial court properly admitted computerized records of Treasury Enforcement Communications System as public records under Rule 803(8) because documents falling under the public records exception are presumed to be trustworthy, and the burden is on the party challenging the records to establish untrustworthiness.)

Rule 803(17) Market Reports, Commercial Publications.

Rule 803(17) recognizes as an exception to the hearsay rule:

“(17) Market reports, commercial publications. Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations.”

This exception covers “lists, etc., prepared for the use of a trade or profession ... newspaper market reports, telephone directories, and city directories. The basis of trustworthiness is general reliance by the public or by a particular segment of it, and the motivation of the compiler to foster reliance by being accurate.” FED.R.EVID. 803(17) advisory committee's note; WEINSTEIN at § 803. 19[1].^{FN53} At least one court has admitted electronically stored compilations and directories under Rule 803(17). Elliott Assoc. L.P. v. Banco de la Nacion, 194 F.R.D. 116, 121 (S.D.N.Y.2000) (finding that plaintiff's expert report properly relied on prime rates of interest obtained from Federal Reserve Board website because they were reliable under Rule 803(17)).

FN53. “[T]he admissibility of market reports and commercial publications under Rule 803(17) is predicated on the two factors of necessity and reliability. Necessity lies in the fact that if this evidence is to be obtained it must come from the compilation, since the task of finding every person who had a hand

in making the report or list would be impossible. Reliability is assured because the compilers know that their work will be consulted; if it is inaccurate, the public or the trade will cease consulting their product.” (citation omitted).

A final observation needs to be made regarding hearsay exceptions and electronic evidence. Rule 802 generally prohibits the admission of hearsay unless one of the exceptions in Rules 803, 804 or 807 apply. What, then, is the effect of hearsay evidence that is admitted without objection by the party against whom it is offered? The general rule is that despite Rule 802, if hearsay is admitted without objection it may be afforded its “natural probative effect, as if it were in law admissible.” New York v. Microsoft, 2002 WL 649951 (“[I]n this country the general rule supported by overwhelming weight of authority is that where ordinarily inadmissible hearsay evidence is admitted into evidence without objection it may properly be considered and accorded its natural probative effect, as if it were in law admissible.”); 3 MICHAEL H. GRAHAM, HANDBOOK OF FEDERAL EVIDENCE § 802.1 (5th ed. 2001) (“In the absence of an objection to hearsay ‘the jury may consider [the hearsay] for whatever natural value it may have; such evidence is to be given its natural probative effect as if it were in law admissible.’ ” (citation omitted)). This underscores the need to pay attention to exhibits offered by an opponent, as much as to those records that you need to introduce. A failure to raise a hearsay objection means that the evidence may be considered for whatever probative value the finder of fact chooses to give it.

In summary, when analyzing the admissibility of ESI for hearsay issues, counsel should address each step of the inquiry in order: does the evidence contain a statement, made by a person, which is offered for its substantive truth, but which does not fall into the two categories of statements identified in 801(d)(1) and 801(d)(2). If, as a result of this analysis, a determination is made that *576 the evidence is hearsay, then it is inadmissible unless it covered by one of the exceptions found in Rules 803, 804 and 807.

If ESI has cleared the first three hurdles by being shown to be relevant, authentic, and admissible under the hearsay rule or an exception thereto, it must also be admissible under the original writing rule before it can

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

be admitted into evidence or considered at summary judgment.

The Original Writing Rule, Rules 1001-1008

The next step in evaluating the admissibility of electronic evidence is to analyze issues associated with the original writing rule, which requires an original or duplicate original to prove the contents of a writing, recording or photograph unless secondary evidence is deemed acceptable.^{FN54} See FED.R.EVID. 1001-08. The best way to understand the rule is to appreciate its structure. Rule 1001 contains the key definitions that animate the rule: “original,” “duplicate,” “writing,” “recording,” and “photograph.” The substantive requirements of the original writing rule are succinctly provided by Rule 1002, which mandates that “[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.” It is Rule 1002 that gives the rule its modern name, the “original writing rule,” as it requires the original to prove the contents of a writing, recording or photograph, except as excused by the remaining rules in Article X of the rules of evidence. As will be seen, the key to the rule is to determine when “the contents” of a writing, recording or photograph actually are being proved, as opposed to proving events that just happen to have been recorded or photographed, or those which can be proved by eyewitnesses, as opposed to a writing or recording explaining or depicting them. Rule 1003 essentially provides that duplicates are co-extensively admissible as originals, unless there is a genuine issue as to the authenticity of the original, or the circumstances indicate that it would be unfair to admit a duplicate in lieu of an original. People v. Huehn, 53 P.3d 733, 738 (Colo.Ct.App.2002) (duplicates of computer generated bank records admissible to the same extent as an original absent unfairness or lack of authenticity). Because of Rule 1003, duplicates are more often admitted into evidence than originals. RICE at 192 (“As a practical matter, Fed.R.Evid. 1003 has eliminated best evidence objections. Copies from the pages of books, treatises, and the other papers are now introduced in place of the entire volume because photocopies of originals are now admissible as if they were the original.”). Rule 1004 is the primary rule that identifies when secondary evidence is admissible. As a practical matter, “secondary evidence” is any proof of the contents of a writing, recording or photograph other than an original or duplicate. Examples include testimony from the author of the writing, or someone

who read it, earlier drafts, copies, or an outline used to prepare the final. Rule 1005 describes how to prove the contents of public records, since it is obvious that something other than the original must be used. Rule 1006 permits introduction into evidence of written or testimonial summaries of voluminous writings, recordings or photographs, provided the original or duplicates from which the summaries were prepared were made available to the adverse party at a reasonable time in advance of trial for examination or copying. Thus, Rule 1006 is an example of secondary evidence. Rule 1007 allows the proof of the contents of a writing, recording or photograph by the deposition or testimony of a party opponent, without having to account for the nonproduction of the original. This is another form of secondary *577 evidence. The final rule in Article X of the Federal Rules of Evidence is Rule 1008. It is a specialized application of Rule 104(b)-the conditional relevance rule-and sets forth what must happen when there is a dispute regarding whether there ever was a writing, recording, or photograph, or when there are conflicting versions of duplicates, originals, or secondary evidence offered into evidence. In such instances, as in Rule 104(b), the jury decides the factual dispute. FED.R.EVID. 1008 advisory committee's note.

FN54. Traditionally the rule has been referred to as the “Best Evidence Rule,” which is a misleading title. The rule is more accurately is referred to as the “Original Writing Rule” because it does not mandate introduction of the “best” evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an “original,” “duplicate” or, in certain instances, by “secondary evidence”—any evidence that is something other than an original or duplicate (such as “testimony, or a draft of a writing to prove the final version, if no original or duplicate is available.”) FED.R.EVID. 1001 advisory committee's note; RICE at 190 (“Article X of the Federal Rules of Evidence codified the common law best evidence rule, terming it instead the original writing rule.”).

It has been acknowledged that the original writing rule has particular applicability to electronically prepared or stored writings, recordings or photographs. One respected commentator has observed:

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

“Computer-based business records commonly consist of material originally produced in a computer (e.g. business memoranda), data drawn from outside sources and input into the computer (e.g. invoices), or summaries of documents (e.g. statistical runs). The admissibility of computer-based records ‘to prove the content of a writing’ is subject to the best evidence rule set out in Rule 1002. The rule generally requires the original of a writing when the contents are at issue, except that a ‘duplicate’ is also admissible unless a genuine issue is raised about its authenticity. A duplicate includes a counterpart produced by ‘electronic re-recording, which accurately reproduces the original.’ Courts often admit computer-based records without making the distinction between originals and duplicates.”

WEINSTEIN at § 900.07[1][d][iv] (citation omitted).

When analyzing the original writing rule as it applies to electronic evidence, the most important rules are Rule 1001, containing the definitions; Rule 1002, the substantive original writing rule; Rule 1004, the “primary” secondary evidence rule; Rule 1006, the rule permitting summaries to prove the contents of voluminous writings, recordings and photographs; and Rule 1007, allowing proof of a writing, recording or photograph by the admission of a party opponent.

Rule 1001 states:

“For purposes of this article the following definitions are applicable:

- (1) Writings and recordings. “Writings” and “recordings” consist of letters, words, or numbers, or their equivalent, set down by handwriting, type-writing, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.
- (2) Photographs. “Photographs” include still photographs, X-ray films, video tapes, and motion pictures.
- (3) Original. An “original” of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An “original” of a photograph

includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original.”

(4) Duplicate. A “duplicate” is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.”

It is apparent that the definition of “writings, recordings and photographs” includes evidence that is electronically generated and stored. *See* FED. RULE EVID. 1001 advisory committee’s note (“Traditionally the rule requiring the original centered upon accumulations of data and expressions affecting legal relations set forth in words and figures. This meant that the rule was one essentially related to writings. Present day techniques have expanded methods of storing data, yet the essential form that the information ultimately assumes for useable purposes is words and figures. Hence, the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments.”). It further is clear that under Rule 1001(3) the “original” of information stored in a computer is the readable display of the information on the computer screen, the hard drive or *578 other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data. WEINSTEIN at § 900.07 [1][d][iv]; RICE at 194; *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind.Ct.App.2002) (ruling that content of internet chat room communications between defendant and undercover police officer that officer “cut-and-pasted” into a word processing program were originals under state version of original writing rule). Moreover, if a computer record accurately reflects the contents of another writing, and was prepared near the time that the original writing was prepared, it may qualify as an original under Rule 1001. *In re Gulph Woods Corp.*, 82 B.R. 373, 377 (Bankr.E.D.Pa.1988) ^{EN55}. *See also* WEINSTEIN at § 900.07[1][d][iv]. Finally, as already noted, as a result of Rule 1003, the distinction between duplicates and originals largely has become unimportant, as duplicates are co-extensively admissible as originals in most instances.

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

FN55. “In today’s commercial world, a single transaction often generates successive entries of the same information in separately prepared writings. Though the purposes of these separate records may be different, a computerized business record, prepared simultaneously with or within a reasonable time period of the written record, and containing the same or similar information, would appear to be no less an ‘original’ than a hand-written record. However, it seems equally clear that where a written record, prepared prior to the computer record, contains a more detailed and complete description of the transaction than that contained in the computer record, the proponent of the evidence should be required to produce the more detailed record, or account for its nonproduction under F.R.E. 1004. Similarly, where a computerized record appears to be nothing more than a summary of a more detailed written record, the written record should be produced except where the requirements of F.R.E. 1006 have been satisfied.” (citations omitted).

Once the definitions of the original writing rule are understood, the next important determination is whether the rule applies at all. Rule 1002 answers this question. It provides: “To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.” As the advisory committee’s note to Rule 1002 makes clear:

“Application of the rule requires resolution of the question whether contents are sought to be proved. Thus an event may be proved by non-documentary evidence, even though a written record of it was made. If, however, the event is sought to be proved by the written record, the rule applies. For example, payment may be proved without producing the written receipt which was given. Earnings may be proved without producing books of account in which they are entered. Nor does the rule apply to testimony that books or records have been examined and found not to contain any reference to a designated matter.

The assumption should not be made that the rule

will come into operation on every occasion when use is made of a photograph in evidence. On the contrary, the rule will seldom apply to ordinary photographs.... On occasion, however, situations arise in which contents are sought to be proved. Copyright, defamation, and invasion of privacy by photograph or motion picture falls into this category. Similarly, as to situations in which the picture is offered as having independent probative value, e.g. automatic photograph of bank robber, photograph of defendant engaged in indecent act.”

FED.R.EVID. 1002, advisory committee’s note (citations omitted); *see also* WEINSTEIN at § 1002.05[1] (“The best evidence rule only applies when the writing, recording or photograph is being introduced ‘to prove the content of a writing, recording or photograph’. The rule is inapplicable when content is not at issue.”)(citing FED.R.EVID. 1002). Whether the content is at issue is determined on a case-by-case basis. *Id.* For example, proof that someone is married may be made by the testimony of a witness to the ceremony. The marriage license is not required. However, the rule applies if the only proof of the marriage is by the record itself. Similarly, someone who heard a politician give a speech may testify to what was said without the video recording of the speech, because the content of the recording is not at issue. In contrast, if the only way to prove the content of the speech is by the video, because there *579 are no witnesses available to testify, the rule would apply to the video recording.

Rule 1002 also does not apply when an expert testifies based in part on having reviewed writings, recordings or photographs, because Rule 703 allows an expert to express opinions based on matters not put into evidence. FED.R.EVID. 1002 advisory committee’s note; WEINSTEIN at § 1002.05[1] (“The best evidence rule does not apply when an expert resorts to material as a basis for an opinion.”). Finally, when the contents of writings, recordings or photographs merely are collateral to the case, meaning they are not “closely related to a controlling issue” in a case, Rule 1002 does not apply, and secondary evidence may be used to prove their contents. FED.R.EVID. 1004(4). In contrast, proving legal transactions, such as wills, contracts, and deeds commonly do involve the best evidence rule because the documents themselves have the central legal significance in the case. WEINSTEIN at § 1002.05[2].

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

An example of when the original writing rule did apply to electronic evidence is *Laughner v. State*, 769 N.E.2d 1147 (Ind.Ct.App.2002), *abrogated on other grounds by Fajardo v. State*, 859 N.E.2d 1201 (Ind.2007). Laughner was charged with attempted child solicitation. To prove the crime, the state offered printouts of instant message chats between the defendant and an undercover police officer posing as a thirteen year old boy. The police officer “cut-and-pasted” the text of the text messages from the internet chat room into a word processing program, and the printouts that were introduced into evidence were prepared from that program. The defendant objected (citing the state version of the original writing rule, which was identical to the federal version), arguing that the printouts were not the “original” of the text of the chat room communications. The appellate court agreed that the state was proving the content of a writing, and that the original writing rule required an original, but found that the printout was an original, reasoning:

“Evidence Rule 1002, the ‘best evidence’ rule, requires an ‘original’ in order to prove ‘the content’ of a writing or recording. However, Evidence Rule 1001(3) provides that when ‘data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is an ‘original.’ According to [the police officer] he saved the conversations with Laughner after they were concluded, and the printout document accurately reflected the content of those conversations. Therefore, the printouts could be found to be the ‘best evidence’ of the conversations [between the defendant and the officer].”

Laughner, 769 N.E.2d at 1159.

It is important to keep in mind that failure to properly object to the introduction of evidence in violation of the original writing rule likely will result in a waiver of the error on appeal. WEINSTEIN at § 1002.04[5][a] (“Procedural safeguards adopted by federal courts also militate against an overtechnical application of the best evidence rule. For example, an appellant’s failure to properly raise an objection to the best evidence rule at trial will result in waiver of the error on appeal.”); *see also State v. Braidic*, 119 Wash.App. 1075, 2004 WL 52412 (2004) (Defendant was convicted of rape and other sex offenses with

minor. At trial, victim’s mother testified, without objection, to content of chat room text messages between defendant and victim. Appellate court noted applicability of original writing rule to require original to prove the contents of the chat room records, but found that defense counsel’s failure to object did not constitute ineffective assistance of counsel). Counsel need to insure that a timely objection is made to attempts to prove the contents of electronic writings, recordings or photographs in violation of the original writing rule, otherwise waiver of the error is the probable consequence.

Rule 1004 identifies four circumstances in which secondary evidence may be introduced instead of an original. The rule provides:

“The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if-

(1) Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or

*580 (2) Original not obtainable. No original can be obtained by any available judicial process or procedure; or

(3) Original in possession of opponent. At a time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing; or

(4) Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue.”

The first example may be particularly suited for electronic evidence. Given the myriad ways that electronic records may be deleted, lost as a result of system malfunctions, purged as a result of routine electronic records management software (such as the automatic deletion of e-mail after a set time period) or otherwise unavailable means that the contents of electronic writings may have to be proved by secondary evidence.^{FNS6} Indeed, at least one court has recognized that the “tenuous and ethereal nature of

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

writings posted in internet chat rooms and message boards means that in all likelihood the exceptions [to the original writing rule that permit secondary evidence] would ... [apply].” *Bidbay.com, Inc. v. Spry*, 2003 WL 723297 (Cal.App.2003)(unpublished opinion); *People v. Huehn*, 53 P.3d 733, 738 (Colo.Ct.App.2002) (holding that trial court did not abuse discretion in admitting computer generated bank records that contained listing of ATM transactions prepared by another company that bank retained to process ATM transactions. The court noted that the Colorado version of Rule 1004(1) permitted secondary evidence of the records provided they were not lost or destroyed in bad faith).

FN56. See, for example, newly revised Fed.R.Civ.P. 37(f), which creates a limited “safe harbor” from sanctions if electronically stored information is not preserved as a result of the routine good faith operation of an electronic records management system. Sanctions may be imposed if the court finds the presence of “extraordinary circumstances” or if it determines that the loss of the ESI was the result of non-routine loss or destruction, or action taken in the absence of good faith. The new rule evidences the widespread recognition that electronically stored information is not infrequently lost or destroyed.

Additionally, Rule 1004 permits proof of the contents of a writing, recording or photograph by secondary evidence when the proponent of the evidence is unable to obtain an original through use of legal process, or when the original is in the possession or control of an adverse party that has actual or inquiry notice of the contents that the proponent intends to introduce the evidence. In the later circumstance, as the advisory committee's note to Rule 104(3) points out, “[a] party who has an original in his control has no need for the protection of the [original writing] rule if put on notice that proof of contents will be made. He can ward off secondary evidence by offering the original.”

Finally, Rule 1004(4) permits proof of the contents of writings, recordings of photographs by secondary evidence if they relate to “collateral matters,” defined as “not closely related to a controlling issue” in the case. The advisory committee's note to Rule 1004(4) candidly acknowledges that this is a nebulous

standard, stating “[w]hile difficult to define with precision, situations arise in which no good purpose is served by production of the original.” See also WEINSTEIN at § 1004.40 (“[t]he distinction between controlling and collateral issues can be an exasperating one. The term ‘collateral’ is elusive and vague. It cannot be defined conceptually, only pragmatically: balancing the importance of the document against the inconvenience of compelling its production, is the rule worth enforcing?”) (citation omitted). An example illustrates. A doctor testifying as an expert in a personal injury case can testify that she is licensed to practice medicine in a state without having to produce the license itself. However, if a defendant is charged with practicing medicine without a license, his testimony alone that he has a license from the state will not be accepted, as the license is closely related to a controlling issue in the case.

Rule 1006 recognizes another source of secondary evidence to prove the contents of writings, recordings, or photographs, stating:

*581 “The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.”

The advisory committee's note recognizes that Rule 1006 is one of necessity, as the “admission of summary of voluminous books, records, or documents offers the only practicable means of making their contents available to judge and jury.” A number of observations may be made about the use of summaries under Rule 1006. First, as the rule expressly states, the writings, recordings or photographs to be summarized must be voluminous. WEINSTEIN at § 1006.03 (“Charts, summaries or calculations are, however, inadmissible when the content being proved is neither voluminous or complicated.”) (citations omitted). Second, although the rule is silent on the nature of the summary, the prevailing view is that it may be either written, or testimonial. *Id.* at § 1006.05[2] (“[s]ummary evidence need not be an exhibit, but may take the form of a witness's oral testimony.”). Third, the majority view is that the summaries themselves constitute the evidence of the contents of the materials

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

summarized, rather than the underlying writings, recordings or photographs. *Id.* at § 1006.04[1] (“[t]he majority rule is that the summary itself is the evidence to be considered by the factfinder when the underlying documents are voluminous and the other requirements of Rule 1006 are met. Other decisions, however, have held that Rule 1006 summaries were not evidence, and that the jury should be so instructed.”). Fourth, if the summaries are accepted as the evidence of the materials summarized, they function as the equivalent of a special exception to the hearsay rule. *Id.* at § 1006.05[4] (“Rule 1006 should be regarded as a special exception to the hearsay rule.”); RICE at 197-98 (Recognizing that summaries of voluminous materials that are introduced to prove the content of the summarized material creates a hearsay problem. The author suggests that the residual hearsay rule, Rule 807, is an exception that may apply to overcome this problem). Fifth, the writings, recordings and photographs that are summarized must be made available to the adverse party for examination or copying reasonably in advance of the use of the summary, a requirement that originates from Rule 1006 itself, regardless of whether the adverse party has served a request for production of documents under FED.R.CIV.P. 34. WEINSTEIN at § 1006.06[1] (“the originals or duplicates of voluminous writings, recordings, or photographs must be made available for examination or copying at a reasonable time or place in order for summary evidence to be admissible. The right to examine the underlying records is absolute. Thus, the records must be made available whether or not the opposing party makes a discovery request for inspection.”). Sixth, the underlying materials from which the summaries are made must themselves be admissible into evidence. *Id.* at § 1006.06[3] (“Charts, summaries and calculations are only admissible when based on original or duplicate materials that are themselves admissible evidence.”).

Because the production of electronically stored information in civil cases frequently is voluminous, the use of summaries under Rule 1006 is a particularly useful evidentiary tool, and courts can be expected to allow the use of summaries provided the procedural requirements of the rule are met. *See, e.g., Wapnick v. Comm’r of Internal Revenue, T.C. Memo. 2002-45, (T.C.2002)* (holding that summaries of voluminous computer records were admissible under Rule 1006 even though they were prepared in anticipation of litigation, because the underlying documents had been admitted into evidence and reasonably had been made

available to the opposing party to inspect).

Rule 1007 identifies another, though little used, way in which secondary evidence may be used to prove the contents of electronically prepared or stored information. It provides that the:

“[c]ontents of writings, recordings, or photographs may be proved by the testimony or deposition of the party against whom offered or by that party’s written admission,*582 without accounting for the non-production of the original.”

On its face this rule is limited to admissions by a party opponent regarding the content of a writing, recording or photograph. Use of the word “admission” refers to any of the types of admissions covered by Rule 801(d)(2), which includes admissions by a representative, agent, employee or co-conspirator that meets the requirements of Rule 801(d)(2) for each of these types of admissions. WEINSTEIN at § § 1007.03[1], 1007.06. It does not require that any showing be made that the writing, recording or photograph is lost or otherwise unavailable. *Id.* at § 1007.04[1]. Further, the rule expressly limits the types of admissions that may be used to prove the contents of writings, recordings or photographs to those obtained during in court testimony, during a deposition, or by the adverse party’s written admission.^{FN57} *Id.* at § 1007.04. An adverse party’s answers to federal rule of civil procedure Rule 33 interrogatories or a Rule 36 request to admit the genuineness of documents would meet the provisions of Federal Rule of Evidence 1007 regarding a “written admission.” *Id.* at § 1007.07 (“[A]n adverse party’s responses to written interrogatories made pursuant to Federal Rule of Civil Procedure 33 are admissible to prove content. Similarly, an adverse party’s responses to requests for admissions made pursuant to Federal Rule of Civil Procedure 36, are admissible to prove contents.”).

^{FN57}. However, despite the limitation in Rule 1007 to testimonial or written admissions of a party opponent, a non-testimonial oral admission by a party opponent would still be admissible as secondary evidence to prove the contents of a writing, recording or photograph under Rule 1004 if the writing, recording or photograph was lost or destroyed, absent bad faith, beyond the reach of court ordered production, in the possession,

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

custody of control of the adverse party, or if the writing, recording or photograph was not closely related to a controlling issue in the litigation. FED.R.EVID. 1007 advisory committee's note ("The limitation [of] Rule 1007 to testimonial or written admissions, of course, does not call for excluding evidence of an oral admission when nonproduction of the original has been accounted for and secondary evidence generally has become admissible."); WEINSTEIN at § 1007.03[1].

Because Rule 1007 so seldom is used or discussed in cases, most lawyers are unaware of it. However, given the frequency with which deponents are asked questions about the content of writings, recordings and photographs, it is prudent to remember that if the deponent is a person whose testimony would qualify as an admission under any of the five varieties recognized by Rule 801(d)(2), then the deposition testimony may be admitted to prove the contents of the writings, recordings and photographs described. The same is true for written responses to FED.R.CIV.P. 33 and 36 discovery that asks for a description of the contents of a writing, recording or photograph. The need is obvious, therefore, to insure that any characterization of the contents of a writing, recording or photograph that could fall within Rule 1007 be accurate.

Rule 1008 is the last of the rules in Article X of the rules of evidence. It states:

"When the admissibility of other evidence of contents of writings, recordings, or photographs under these rules depends upon the fulfillment of a condition of fact, the question whether the condition has been fulfilled is ordinarily for the court to determine in accordance with the provisions of rule 104. However, when an issue is raised (a) whether the asserted writing ever existed, or (b) whether another writing, recording, or photograph produced at the trial is the original, or (c) whether other evidence of contents correctly reflects the contents, the issue is for the trier of fact to determine as in the case of other issues of fact."

This rule is a specialized application of Rule 104(b), and it allocates responsibility between the trial judge and the jury with respect to certain preliminary matters affecting the original writing rule. As the advisory committee's note to Rule 1008 states:

"Most preliminary questions of fact in connection with applying the rule preferring the original as evidence of contents are for the judge, under the general principles announced in Rule 104(a). Thus, the question whether the loss of the originals has been established, or of the fulfillment of other conditions specified in Rule 1004, *583 supra, is for the judge. However, questions may arise which go beyond the mere administration of the rule preferring the original and into the merits of the controversy ... The latter portion of [Rule 1008] is designed to insure treatment of these situations as raising jury questions. The decision is not one for uncontrolled discretion of the jury but is subject to the control exercised generally by the judge over jury determinations. See Rule 104(b)."

See also WEINSTEIN at § 1008.02[1]-1008.04[5]. Under the rule, the trial judge determines: whether originals have been lost or destroyed under Rule 1004(1), as well as all issues relating to the appropriateness of the proponent's efforts to search for the lost original; ^{FN58} whether or not the original is obtainable by judicial process, under Rule 1004(2); ^{FN59} whether the original is in the possession, custody or control of the opposing party under Rule 1004(3); ^{FN60} and whether the writing, recording or photograph relates to a collateral matter, which removes it from the reach of the original writing rule. ^{FN61}

FN58. WEINSTEIN at § 1008.04[3]

FN59. *Id.* at § 1008.04[4]

FN60. *Id.* at § 1008.04[5]

FN61. *Id.* at § 1008.04[6]

Rule 1008 identifies three issues that are questions for the jury, however: (1) whether the writing, recording or photograph ever existed in the first place; (2) whether some other writing, recording, or photograph that is offered into evidence is in fact the original; and (3) whether "other" (i.e. secondary) evidence of contents correctly reflects the content of the writing, recording or photograph. FED.R.EVID. 1008 advisory committee's note; WEINSTEIN at § 1008.05[1]. Counsel need to be aware of the different functions the judge and jury serve as they anticipate how to offer electronic writings, recordings and pho-

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

tographs into evidence. Given the challenges that often are associated with the authentication of electronically created or stored evidence, it is not unlikely that there will be disputes of fact regarding whether an electronic writing ever existed in the first place, if the original cannot be produced and secondary evidence is offered, or when different versions of the same electronic document are offered into evidence by the opposing parties.

In summary, when counsel intend to offer electronic evidence at trial or in support of a motion for summary judgment they must determine whether the original writing rule is applicable, and if so, they must be prepared to introduce an original, a duplicate original, or be able to demonstrate that one of the permitted forms of secondary evidence is admissible. In this case, counsel did not address the original writing rule, despite its obvious applicability given that the e-mail exhibits were closely related to a controlling issue and there were proving the contents of the e-mails themselves.

The final evidentiary issue that must be considered in determining whether electronic evidence will be admitted is whether the probative value of the evidence is substantially outweighed by the danger of unfair prejudice, as proscribed under Rule 403 of the federal rules of evidence.

Balancing Probative Value Against the Danger of Unfair Prejudice Under Rule 403

After evaluating the issues associated with relevance, authenticity, hearsay, and the original writing rule, the final step to consider with regard to electronically prepared or stored evidence is the need to balance its probative value against the potential for unfair prejudice, or other harm, under Rule 403 of the Federal Rules of Evidence. This rule states:

“Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.”

FED.R.EVID. 403. The advisory committee note to Rule 403 succinctly explains its function:

“[C]ertain circumstances call for the exclusion of evidence which is of unquestioned relevance. These

circumstances entail *584 risks which range all the way from inducing decision on a purely emotional basis, at one extreme, to nothing more harmful than merely wasting time, at the other extreme. Situations in this area call for balancing the probative value of and need for the evidence against the harm likely to result from its admission.... ‘Unfair prejudice’ within its context means an undue tendency to suggest decision on an improper basis, commonly, though not necessarily an emotional one.”

See also WEINSTEIN at § 403.02[1][a].^{FN62}

FN62. “Rule 403 recognizes that relevance alone does not ensure admissibility. A cost/benefit analysis must often be employed. Relevant evidence may be excluded if its probative value is not worth the problems that its admission may cause. The issue is whether the search for truth will be helped or hindered by the interjection of distracting, confusing, or emotionally charged evidence.”

A determination of whether evidence should be excluded under Rule 403 falls within the those made by the court under Rule 104(a), but it is used sparingly. WEINSTEIN at § 403.02[2][a]. Generally, “[i]f there is doubt about the existence of unfair prejudice, confusion of issues, misleading, undue delay, or waste of time, it is generally better practice to admit the evidence, taking necessary precautions of contemporaneous instructions to the jury followed by additional admonitions in the charge.” *Id.* at § 403.02[2][c].

Although Rule 403 may be used in combination with any other rule of evidence to assess the admissibility of electronic evidence, courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in the following circumstances: (1) When the evidence would contain offensive or highly derogatory language that may provoke an emotional response. See Monotype Corp., 43 F.3d at 450 (Finding that trial court properly excluded an email from a Microsoft employee under Rule 403 that contained a “highly derogatory and offensive description of ... [another company's] type director.”); (2) When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation, Friend v. Time Manufacturing Co., 2006 WL

241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446
(Cite as: 241 F.R.D. 534)

2135807 at *7 (D.Ariz.2006) (“Therefore, the question is simply whether the animation accurately demonstrates the scene of the accident, and whether the probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.”); State v. Sayles, 662 N.W.2d 1, 11 (Iowa, 2003) (Appellate court found no error in trial court’s admission of computer animation slides showing effects of shaken infant syndrome, finding that trial court properly considered state version of Rule 403, and admitted evidence with a cautionary instruction that the evidence was only an illustration, not a re-creation of the actual crime); (3) when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 1006, WEINSTEIN at § 1006.08[3] (“Summary evidence is subject to the balancing test under Rule 403 that weighs the probative value of evidence against its prejudicial effect.”); and (4) In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence, St. Clair v. Johnny’s Oyster and Shrimp Inc., 76 F.Supp.2d 773 (S.D.Tx.1999) (Court expressed extreme skepticism regarding the reliability and accuracy of information posted on the internet, referring to it variously as “voodoo information”. Although the court did not specifically refer to Rule 403, the possibility of unfair prejudice associated with the admissibility of unreliable or inaccurate information, as well as for confusion of the jury, makes Rule 403 a likely candidate for exclusion of such evidence).

Thus, when a lawyer analyzes the admissibility of electronic evidence, he or she should consider whether it would unfairly prejudice the party against whom it is offered, confuse or mislead the jury, unduly delay the trial of the case, or interject collateral matters into the case. If a lawyer is offering electronic evidence, particularly computer animations, that may draw a Rule 403 objection, he or she must be prepared to demonstrate why any prejudice is not unfair, when measured against the probative value of the evidence. *585 In this case, counsel did not address whether Rule 403 was implicated with respect to the electronic evidence attached to their summary judgment memoranda.

Conclusion

[3] In this case the failure of counsel collectively

to establish the authenticity of their exhibits, resolve potential hearsay issues, comply with the original writing rule, and demonstrate the absence of unfair prejudice rendered their exhibits inadmissible, resulting in the dismissal, without prejudice, of their cross motions for summary judgment. The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try. The Court hopes that the explanation provided in this memorandum order will assist in that endeavor.^{FN63}

FN63. I acknowledge with gratitude the tireless assistance of two exceptionally talented law student interns, Ms. Puja Gupta and Mr. Ben Peoples, whose assistance in cite checking was invaluable, and my law clerk, Ms. Kathryn Widmayer, who consistently makes the most difficult tasks appear easy.

D.Md.,2007.
Lorraine v. Markel American Ins. Co.
241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446

END OF DOCUMENT

American Law Institute - American Bar Association Continuing Legal Education
ALI-ABA Course of Study
July 28 - 30, 2011

Current Developments in Employment Law: The Obama Years at Mid-Term

*1287 CASES DISCUSSING SOCIAL MEDIA -- EMPLOYMENT ISSUES, DISCOVERY, ADMISSIBILITY,
AUTHENTICATION, AND ETHICS -- MAY 2011

Paul W. Grimm
U.S. District Court
Baltimore, Maryland

Copyright (c) 2011 The American Law Institute; Paul W. Grimm

CASE

DISCUSSION

[cases not related to social media were deleted]

Admissibility and Authentication of Social Media Contents

Griffin v. State, No. 74, 2011 WL 1586683 (Md. April 28, 2011) (Considering '[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user,' the court concluded that a printout from a social media site 'requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site' to determine that the person whose birthday is listed and whose photograph appears on the site is both the creator of the site and the person who wrote the posting. Social media site content can be authenticated through, for example, the person who allegedly created the page and the posting; the internet history of that person's computer, if it shows that the computer was used to make the page and the posting; and the social networking website, if it can provide information linking the profile and posting to the person who allegedly made them)

At trial, the State offered printouts from the defendant's girlfriend's MySpace profile, on which the statement 'FREE BOOZY [defendant's nickname]!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!' appeared, to show that the girlfriend, Ms. Barber, had threatened another State witness prior to trial by posting that statement on her profile. *Id.* at *1. Outside the jury's presence, the State offered testimony from its lead investigator (but not from the girlfriend) in an 'attempt[] to authenticate the pages, as belonging to [the girlfriend].' *Id.* The investigator testified that he knew it was the girlfriend's page '[t]hrough the photograph of her and Boozy on the front, through the reference to Boozy, [] the reference [to] the children, and [] her birth date indicated on the form.' *Id.* at *2. Defense counsel objected to the evidence 'because the State could not sufficiently establish a 'connection' between the profile and posting and Ms. Barber,' but the trial court admitted the printouts. *Id.* at *1-2.

Defendant appealed, alleging that the printouts were inadmissible because they were not properly authenticated. *Id.* at *1. The Court of Appeals reversed and remanded, *id.* at *1, holding that 'the picture of Ms. Barber, coupled with her birth date and location, were not sufficient 'distinctive characteristics' on a MySpace profile to authenticate its printout [pursuant to Md. Rule 5-901, which is materially similar to Fed. R. Evid. 901], given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the 'snitches get stitches' comment.'

Id. at *6.

Quoting *Lorraine*, 241 F.R.D. at 541-44, the court stated that ‘the ‘requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims,’ to insure trustworthiness,’ and ‘authenticating electronically stored information presents a myriad of concerns because ‘technology changes so rapidly’ and is ‘often new to many judges’ and ‘requires greater scrutiny of ‘the foundational requirements’ than letters or other paper records, to bolster reliability.’ *Id.* at *6. The court observed that ‘[t]he identity of who generated the profile may be confounding, because ‘a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate,’ and, with ‘relative ease,’ a person ‘can create a fictitious account and masquerade under another person’s name or can gain access to another’s account by obtaining the user’s username and password.’ *Id.* at *4 (citation omitted).

Considering ‘[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user,’ the court concluded that a printout from a social media site ‘requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site’ to determine that the person whose birthday is listed and whose photograph appears on the site is both the creator of the site and the person who wrote the posting. *Id.* at *6. The court suggested proper means to authenticate printouts of postings on social media sites: (1) ‘the purported creator if she indeed created the profile and also if she added the posting in question’; (2) ‘search the computer of the person who allegedly created the profile and posting and examine the computer’s internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question’; and (3) ‘obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it.’ *Id.* at *9-10.

The dissent stated that, given the investigator’s testimony and the website’s contents, ‘a reasonable juror could conclude . . . that the redacted printed pages of the MySpace profile contained information posted by Ms. Barber,’ and a document should be properly authenticated ‘if a reasonable juror could find in favor of authenticity.’ *Id.* at *10 (Harrell, J., dissenting).

positively identified)

injury. *Id.* at *5-6. At trial, Husband offered (as statements against interest) and Wife 'positively identified' printouts from Wife's internet blogs, which discussed Wife's frequent belly dancing and showed photos of Wife belly dancing, as well as printouts of comments Wife posted to her Facebook page about her belly dancing. *Id.* Wife stated the screen name she used on tribe.net, facebook.com, and myspace.com and 'admitted that the contents of what she posted on the internet [were] true.' *Id.* at *5. The court noted that '[a]t trial, Wife incredibly testified that she stopped belly dancing in 2008, notwithstanding her own blogs which reveal otherwise.' *Id.* In determining whether to award maintenance, the court relied on 'Wife's admissions in her blogs' as proof that 'she can spend significant time on a computer and is physically capable of traveling into Manhattan to belly dance on a frequent basis.' *Id.* at *16.

LaLonde v. LaLonde, No. 2009-CA-2279-MR, 2011 WL 832465 (Ky. Ct. App. Feb. 25, 2011) (opponent's own testimony properly authenticating pictures by acknowledging that they were what they were alleged to be)

In custody dispute, trial court admitted Facebook pictures of mother. *Id.* at *2. Mother appealed decision to award physical custody to father, arguing that the commissioner partially based his decision on the Facebook pictures, which were improperly admitted because they were not properly authenticated. *Id.* Citing the state equivalent to Fed. R. Evid. 901, the appellate court held that pictures were properly authenticated because the mother 'acknowledged that indeed, she had been drinking alcohol and the pictures accurately reflected that activity.' *Id.* It said: 'That testimony was sufficient to authentic the photographs and they were properly admitted into evidence.' *Id.*

Commonwealth v. Williams, 926 N.E.2d 1162 (Mass. 2010) (testimony about MySpace messages should not be admitted without adequate foundation that identified who sent the messages, not only the account from which they were sent; printouts of the MySpace page not admitted)

At trial in a case regarding a shooting death, a witness testified that the defendant was carrying a handgun on the evening of the murder. *Id.* at 1172. The witness also testified that the defendant's brother had the MySpace screen name 'doit4it' and had a photo of himself on his MySpace page. *Id.* The witness said that, through four instant messages on her MySpace page that the defendant's brother sent to her using the screen name 'doit4it,' the defendant's brother told her 'not to testify or to claim a lack of memory regarding the events of the night of the murder.' *Id.* The trial court admitted, over defendant's objection, the witness's testimony about the messages, although it did not admit printouts of the MySpace page. *Id.* at 1171 & n.9.

The appellate court analogized the MySpace messages to a phone call, stating that 'a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.' *Id.* at 1172. Noting that the State did not offer any evidence about 'how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc.,' the court held that the trial court should not have admitted testimony about the messages because the State failed to lay an adequate

foundation to authenticate the MySpace messages. *Id.* It concluded that, 'while the foundational testimony established that the messages were sent by someone with access to [the defendant's brother's] MySpace Web page, it did not identify the person who actually sent the communication.' *Id.* at 1172-73. The court added that there also was no 'expert testimony that no one other than [the defendant's brother] could communicate from that Web page.' *Id.* at 1173.

People v. Lenihan, 911 N.Y.S.2d 588 (N.Y. Sup. Ct. 2010) (MySpace photos not admitted because defendant could not authenticate them; authenticity concerns included ability to photoshop, questions of who took the photos and who posted them)

Post-conviction, the defendant moved to set aside the verdict, alleging that the court erred and violated his right to confrontation when it would not allow him to use photographs printed from MySpace to cross-examine two witnesses. *Id.* at 591. The photographs showed the witnesses and the victim 'making hand gestures and wearing articles of clothing that suggest an affiliation with the 'Crips' gang.' *Id.* The court held that it did not err because, '[i]n light of the ability to 'photo shop,' edit photographs on the computer, defendant could not authenticate the photographs.' *Id.* at 592. Also, 'Defendant did not know who took these photographs or posted them on 'Myspace.' *Id.* at 591.

People v. Clevestine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009) (under the circumstances, MySpace messages properly authenticated via testimony of authors of some of the messages, police officer who retrieved data from computer hard drive, and MySpace employee)

At trial, the State offered into evidence a computer disk containing instant messages exchanged on MySpace between the defendant and his victims, whom he allegedly raped. *Id.* at 514. The defendant objected, alleging that the evidence 'had not been properly authenticated.' *Id.* The trial court admitted the evidence, the defendant appealed. *Id.* at 513-14.

The appellate court said that 'authenticity is established by proof that the offered evidence is genuine and that there has been no tampering with it,' and '[t]he foundation necessary to establish these elements may differ according to the nature of the evidence sought to be admitted.' *Id.* at 514 (quoting *People v. McGee*, 399 N.E.2d 1177 (1979)). It affirmed, holding that there was 'ample authentication for admission of this evidence.' *Id.* at 514. It noted:

[B]oth victims testified that they had engaged in instant messaging about sexual activities with defendant through the social networking site MySpace, an investigator from the computer crime unit of the State Police related that he had retrieved such conversations from the hard drive of the computer used by the victims, a legal compliance officer for MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by defendant and the victims, and defendant's wife recalled the sexually explicit conversations she viewed in defendant's MySpace account while on their computer.

Id. The appellate court acknowledged that ‘it was possible that someone else accessed his MySpace account and sent messages under his user name,’ but said that the trial court ‘properly concluded that, under the facts of this case, the likelihood of such a scenario presented a factual issue for the jury.’ *Id.*

Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) (discussing authentication of ESI generally and website content specifically; focusing on Rules 901 and 902)

The court comprehensively discussed ‘the evidentiary issues associated with the admissibility of electronically generated and stored evidence,’ including authentication under Rules 901-02, in an analysis that the *Griffin* court applied to authentication of social media site contents. *Id.* at 537. The court addressed the judge-jury relationship and Rule 104; relevance under Rule 401; hearsay under Rules 801-807; whether the evidence offered is an original under the original writing rule, considering Rules 1001-08; and the balancing test required by Rule 403. *Id.* at 538. The court noted that the authentication requirement ‘as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.’ *Id.* at 541-42 (quoting Rule 901(a)). It explained that ‘[t]his is not a particularly high barrier to overcome,’ as ‘[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,’ and ‘[t]he court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury might ultimately do so.’ *Id.* at 542 (citation omitted).

The court observed that Rule 901(b) provides a non-exclusive list of means of authenticating ESI, and that courts have employed 901(b)(1) (testimony of a witness with ‘personal knowledge of how that type of exhibit is routinely made’ who provides ‘factual specificity’ about how the ESI ‘is created, acquired, maintained, and preserved without alteration or change,’ or about how it is produced via ‘a system or process that does so’; it is not sufficient for witness to provide ‘boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule . . . or public record exception’), (3) (comparison to authenticated documents), (4) (consideration of circumstances and distinctive characteristics of the document, e.g. hash values and metadata), (7) (showing, for public records, that ‘the office from which the records were taken is the legal custodian of the records’), and (9) (‘proof that [the records] were produced by a system or process capable of producing a reliable result’). *Id.* at 544-49. Additionally, the court noted that Rule 902 provides for self-authentication (sometimes with an accompanying certificated signed by a custodian) of certain enumerated documents such as, *inter alia*, public documents, official publications, trade inscriptions, and certified domestic records of regularly conducted activity. *Id.* at 550-51. It stated that ‘the court admitted into evidence printouts of

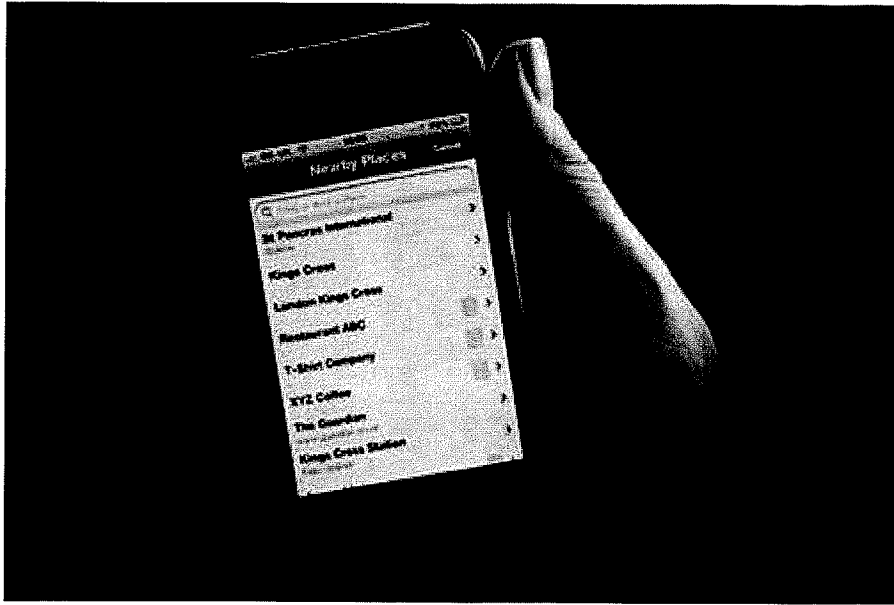
postings on the website of the United States Census Bureau as self-authenticating under Rule 902(5)' in *Equal Employment Opportunity Commission v. E.I. DuPont de Nemours & Co.*, 2004 WL 2347556 (E.D. La. Oct.18, 2004). *Id.* at 551. However, it cautioned that the opposing party still may challenge the authenticity of the document, in which case 'exhibit and the evidence challenging its authenticity goes to the jury, which ultimately determines whether it is authentic.' *Id.* Judicial notice under Rule 201 could be useful in authenticating ESI. *Id.* at 553.

With regard to website postings specifically, the court noted that one concern is whether 'the organization hosting the website actually posted the statements or authorized their posting.' *Id.* at 555. It said that, '[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (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?' *Id.* (citation omitted). Other factors relevant to the admissibility of website postings as evidence, and which counsel should consider when deciding how to build a foundation and authenticate the evidence, include:

'The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question?'

Id. at 555-56 (citation omitted). The court stated that the 'authentication rules most likely to apply, singly or in combination,' to website postings are Rules 901(b)(1), (3), (4), (7), and (9), and 902(5) (official publications).

Facebook Creeps Into Courtrooms



BY MARGARET ROCK | TUE FEB 22, 2011 12:04 PM

Facebook is changing the courtroom, playing an increasing role in jury selection and causing legal complications.

Prosecutors and defense attorneys are scouring Facebook and Twitter to see what potential jurors watch on television, their interests and hobbies and how religious they are -- information that's more useful than what they can get from standard questionnaires.

But the practice of investigating possible jurors' social networking profiles is controversial. In some places, the courts have upheld the lawyers' rights to research jurors online. Recently, a New Jersey Appellate Court ruled that a lower court judge erred by prohibiting a plaintiff's attorney from using the Internet in the courtroom.

But others don't think the courts should abandon the traditional jury selection process in favor of Internet snooping.

"There are a number of people who post who they want to be, as opposed to who they are," said Jason Schultz, co-director of the Samuelson Law, Technology and Public Policy Clinic at the University of California at Berkeley Law School.

Facebook use by jurors has also come under scrutiny.

"Back to jury duty can it get any more BORING than going over piles and piles of metro

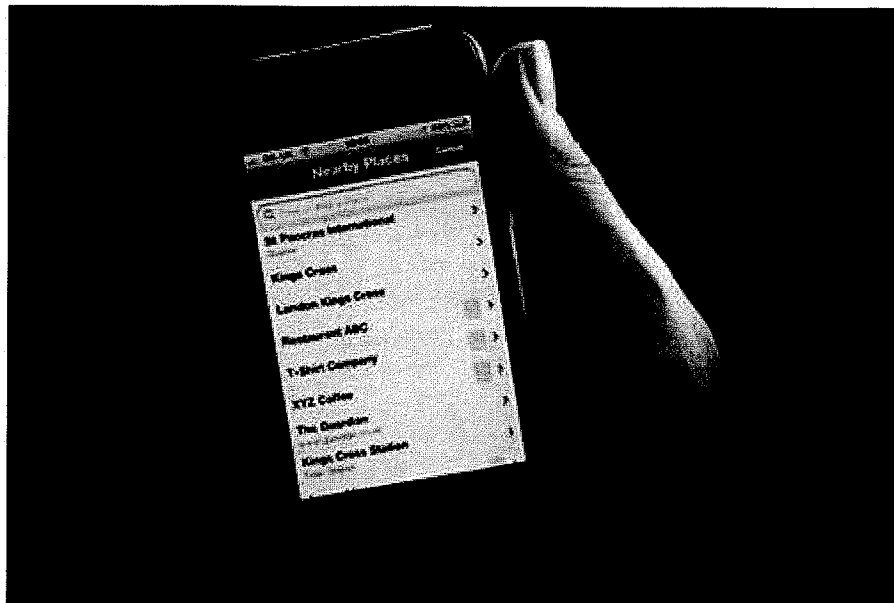
pcs phone records... uuuuughh," Arturo Ramirez, a jury foreperson posted to Facebook in 2008.

After the trial concluded and the jury delivered a conviction on the gang beating case, defense attorneys found out about the posting and issued subpoenas to Facebook and Ramirez for records of the status update. The social networking website initially refused, but last week the court ordered Ramirez to sign a consent order allowing Facebook to hand over the posting.

The order was appealed, and subsequently denied, by the California Court of Appeals, and the case is currently awaiting review by the California Supreme Court.

As Facebook penetrates into all aspects of modern life, its usage in courthouses, jury rooms and legal cases will only continue -- and continue to attract controversy.

Police, Prosecutors Look for Evidence on Facebook, Twitter



BY DOUG RULE | THU MAR 03, 2011 1:51 PM

Watch what you type: police and prosecutors are increasingly using Facebook and Twitter for evidence to prosecute crimes and investigate fraud.

Prosecutors, especially those focused on criminal gangs, can look to social media like Twitter, Facebook and Foursquare to prove connections between people, offering building blocks for a case.

In the case of the January Arizona shooting rampage focused on U.S. Rep. Gabrielle Giffords, prosecutors may use the "Goodbye friends" message alleged gunman Jared Loughner posted to MySpace hours before the crime as evidence against him.

Even benign postings can help, or hurt, a case. The New York Times reported on a boy who had been charged with a robbery in Brooklyn -- until his Facebook posting, jokingly complaining about breakfast at his dad's house in Manhattan, supported his claims that he was otherwise engaged at the time of the crime. The charges were dropped.

It's not just law enforcement that mining social media for evidence. Health insurers, especially those focused on disability, medical liability and workers' compensation, are regularly monitoring Facebook and Twitter to detect fraud. A 23-year-old Floridian who claimed to be disabled by injuries from an auto accident was caught out by investigators, thanks to his regular tweeting about extreme jet skiing adventures.

"Insurance companies and representatives of insurance companies are using social media to get an edge on their competition in understanding the risk profile of the insured," said Owen Tripp, co-founder and chief operating officer of online profile management firm Reputation.com.

Social media not only has found its way into the evidence-gathering of prosecutors, but has also made inroads into the legal process itself. Lawyers are increasingly sifting through the postings, messages and

check-ins on social networking sites to determine jury selection.

As social media redefines boundaries between public and private, people who misinterpret that shifting line are finding their private worlds becoming unexpectedly public.

Although catching criminals and cheats is a handy byproduct of this confusion, their self-incrimination highlights the need for both individuals and social network designers to think carefully about how we handle our online lives.

Does Facebook Ruin Marriages? It's Complicated



BY DOUG RULE | WED MAR 09, 2011 7:09 PM

As many as one in five divorce cases mention Facebook as the primary source of tension, according to the American Academy of Matrimonial Lawyers.

A report by the AAML found that postings and photographs from the social network site provide more damning evidence of infidelity or lies about activities than any other source. Lawyers are increasingly demanding to see clients' Facebook pages to use such evidence in divorce proceedings, suggesting that social media is becoming a way to gauge trust and truthfulness.

"If you publicly post any contradictions to previously made statements and promises, an estranged spouse will certainly be one of the first people to notice and make use of that evidence," said Marlene Eskind Moses, the AAML's president.

In fact, four out of five lawyers report that evidence derived from social media sites has increased dramatically in the past five years, according to a recent AAML survey. Of course, collecting such evidence was harder, if not impossible, before the widespread adoption of sites like Facebook that can keep records and expose people's private lives.

Facebook doesn't appear to be contributing to a rise in the divorce rate, which is actually declining slightly, mostly due to fewer people getting married than getting divorced. Sites such as Facebook are clearly complicating relationships as much as they're nurturing them, but ultimately whatever damage they cause is insult to injury. They simply reveal a troubled relationship's lack of trust and honesty.

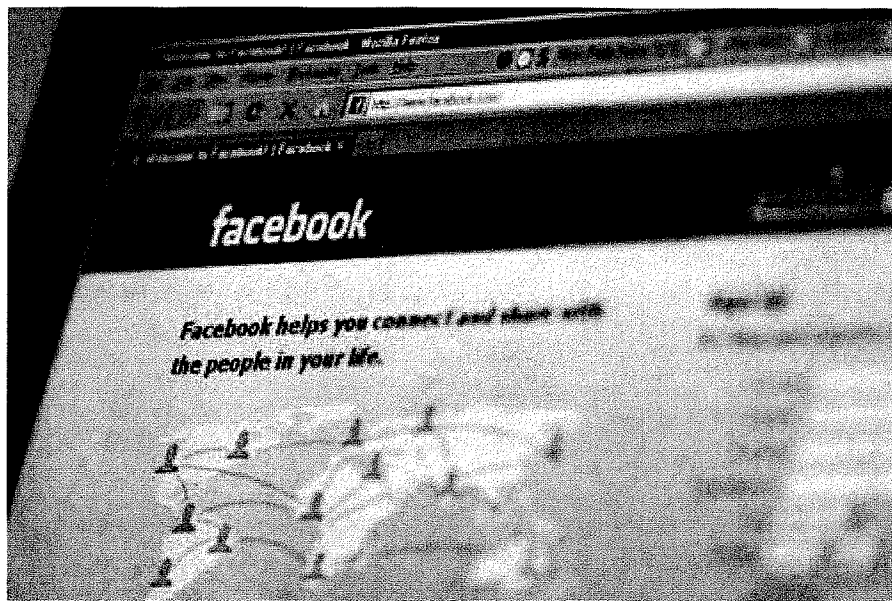
Perhaps revealing the wide lead Facebook holds in social networking, only about 14 percent of divorce cases involve MySpace and just 5 percent Twitter.

Lawyers aren't the only ones snooping online. Police, prosecutors and health insurers are increasingly mining social media for evidence to prosecute crimes and investigate fraud. Lawyers are even

increasingly sifting through the postings, messages and check-ins on social networking sites to determine jury selection.

Nielsen statistics reveal that 135 million people in the U.S. visited Facebook during the month of January, or nearly 70 percent of Internet users.

Facebook Firing Lawsuit Settled



BY EMILY ANDERSON | TUE FEB 08, 2011 12:24 PM

A Connecticut company that fired an employee after she made negative comments about her boss on Facebook has agreed to rework its rules so workers' rights are protected following a complaint over the firing.

The complaint, filed with the National Labor Relations Board, has been settled, along with a private agreement between the ex-employee, Dawnmarie Souza, and the company, American Medical Response of Connecticut. The result of the private settlement has not been divulged.

Souza was fired after complaining on the social networking site that her boss illegally denied her union representation during an investigation about a customer complaint. The comment drew support from co-workers and further negative comments from Souza about the supervisor.

Souza's firing in fall 2010 was ruled illegal by the board because they said posting comments on Facebook counted as "protected concerted activity" -- speech protected under the National Labor Relations Act.

The board found AMRC's rules about Internet behavior to be vague, and the company has agreed to change its rules so employees can freely discuss wages and other job-related issues on the Web without fear of discipline or losing their jobs.

"The fact that they agreed to revise their rules so that they're not so overly restrictive of the rights of employees to discuss their terms and conditions with others and with their fellow employees is the most significant thing that comes out of this," said Jonathan Kreisberg, NLRB Regional Director in Hartford, Conn.

Facebook-related firings are nothing new, and neither are lawsuits related to those firings. Ashley Payne of Georgia said she was forced to resign as a high school teacher after a picture of her holding a glass of

wine on vacation appeared on the social networking site, for example.

AMRC also agreed to approve all employee requests for union representation from now on.

Facebook in Divorce Court



BY EMILY ANDERSON | MON APR 25, 2011 12:55 PM

Facebook is playing a role in divorce cases and custody battles, as users continue to underestimate their exposure online where the line between public and private are increasingly blurred.

Leading attorneys reportedly advise clients to refrain from making disparaging remarks about their soon-to-be-ex-spouse or any professional involved in divorce proceedings on Facebook because the postings could be used in court.

Legal blog Rhode Island Divorce Lawyers Articles recently noted even if a person doesn't think their ex-spouse is watching for comments that could be used as evidence a person is cheating, a bad parent or simply uncooperative, a Facebook "friend" could be watching for them.

An Indianapolis ABC news station recently interviewed a Marion County, Ind. judge, Cynthia Ayers, who told the station that social media is "playing a bigger and bigger role all the time" in custody and child protection cases.

"I saw a picture of a toddler in front of a coffee table with bags of marijuana, whiskey bottles and a big pile of money," said Janice Davidson, director of the Marion County Domestic Relations Counseling Bureau, to the station. "We called Child Protective Services and got them involved so they could make sure that child was protected."

In March, the American Academy of Matrimonial Lawyers found that 80 percent of divorce cases included social media posts, mostly from Facebook, as evidence in the past five years.

Taken in context with a host of examples of supposedly-private social media turning into damaging evidence, it's clear that social media is increasingly just an extension of society, and that people continue to think they have more control over who sees their social content than they actually do.

It's not just in the courtroom where the supposed private revelations of social networking affect more public aspects of lives. Other recent cases illustrate how the culture is still trying to navigate the divide between the public and private aspects of social media.

Georgia school teacher Ashley Payne was asked to resign from her job two years ago after she posted a photo of herself drinking alcohol on vacation on her Facebook page -- despite the fact that there's no law saying teachers can't drink on vacation.

In some cases, those accused of Facebook naughtiness have successfully fought back. Dawnmarie Souza, a medic fired last year after she posted disparaging remarks about her employer, later won a settlement from the company from the National Labor Relations Board.

Facebook Search Warrants on the Rise



BY MARGARET ROCK | WED JUL 13, 2011 10:57 AM

U.S. law enforcement can obtain warrants to search Facebook for detailed access to account information without users' knowledge, another example of the social network's increasing role in the legal world.

A Reuters review of the Westlaw legal database reveals that federal judges authorized at least two dozen warrants to search Facebook accounts, including messages, status updates, links to videos and photographs, calendars of events, wall postings and friend requests. And, in the first half of 2011, they issued almost twice as many as they did in all of 2010.

Federal agencies like the FBI, DEA and ICE seek warrants, which typically demand a Facebook user's "Neoprint" and "Photoprint." These are terms Facebook uses to refer to profile and picture packages that contain information not even available to users themselves.

To complete the search warrants, law enforcement follows guidelines outlined in manuals reportedly put together by Facebook, though the social network officials won't confirm their authenticity.

Facebook's chief security officer Joe Sullivan declined to comment in a telephone interview on how many warrants had been served on the company, but stressed Facebook is sensitive to user privacy and regularly pushes back against law-enforcement "fishing expeditions."

The news comes amidst growing awareness that all sorts of business, commercial and legal interests leverage social media to gain information about their users. For example, alleged gunman Jared Loughner posted on MySpace hours before he embarked on the shooting rampage that seriously wounded Arizona's Representative Gabrielle Giffords; his posts may be used as evidence against him in the pending case.

In addition to helping build criminal cases, debt collectors, divorce attorneys, and even fraud investigators are combing through Facebook and gathering information to pursue their cases.

So far, no court has challenged the Facebook warrants nor said they violate Fourth Amendment protections against unlawful search and seizure.

That may be because, by law, neither Facebook nor the government has an obligation to inform users when their accounts are subject to search, or to notify users' "friends" whose posts and pictures may have been searched as well.

But if a case is filed against a user, prosecutors must disclose material evidence to a defendant, including any information gleaned on the social networking site. This is similar to current laws governing banks and other institutions.

Twitter, while subject to the same laws, has adopted a policy to notify users when law enforcement asks to search their profiles. This past January, the social media service challenged a gag order and won.

The Facebook spokesman didn't say whether the company had a similar policy for notifying users, or if it was considering one.

The federal courts have skirted debates on privacy protections of late. The Supreme Court demurred from addressing the privacy expectations of digital data head-on when it ruled in a recent case.

Explaining the court's caution and hinting it may tackle the topic another day, Justice Anthony Kennedy wrote, "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

Fugitive Caught Posing With Obama Waxwork

Updated: Sunday, 12 Feb 2012, 11:12 AM EST
Published : Sunday, 12 Feb 2012, 11:12 AM EST

(NewsCore) - An Italian fugitive was caught after years on the run when he posted a photo on Facebook showing himself posing with a wax model of US President Barack Obama, the ANSA news agency reported.

Michele Grasso, a 27 year old from Sicily, disappeared in 2008 to escape a conviction for drug dealing. He ended up in London, where he found work in an Italian restaurant.

But a trip to the famous Madame Tussauds wax museum in the British capital proved his undoing, after he posted online a photo of himself standing next to a grinning model of Obama.

Italian police, who monitored his Facebook account, immediately suspected he was in London. Another photo showed him working as a waiter at a restaurant, which was enough to set the wheels in motion to track him down.

Italian cops contacted their British counterparts, who found Grasso in a London suburb. The report did not say when the arrest and subsequent deportation took place.

Grasso was arrested upon arrival in the Italian capital Rome, and transferred to prison to start his five-year sentence.

Facebook Helps Prosecutors Charge Alleged Attempted Burglars

Wednesday February 1, 2012 5:49 PM
UPDATED: Wednesday February 1, 2012 10:03 PM

COLUMBUS, Ohio - Two people faced burglary charges on Wednesday after a search warrant led investigators to an incriminating Facebook message.

Kevin Stoll II and Meghan Welch allegedly were involved in a burglary, and investigators said that Welch sent a message to a friend saying, "That guy in the picture robbed a house, and I was in the car, so I got charged with burglary," 10TV's Maureen Kocot reported.

According to Franklin County prosecutor Ron O'Brien, Facebook can be an invaluable tool for investigators.

"People just have a habit of talking too much too often in the wrong place," O'Brien said.

In September, police charged a woman with felonious assault after investigators said that she smashed a glass into a woman's face.

The victim sued Courtney Tomlinson after attorneys said that she bragged on Facebook saying, "I cut my thumb bad on some glass and had to get a few stitches and sure enough, she was there, too, getting her face stitched up."

Prosecutors also filed charges against 19 suspected gang members who said that they did not know each other, but when investigators looked at their Facebook accounts, they found pictures of the people together, Kocot reported.

"And of course, if you have a picture of them flashing gang signs together and smiling and holding guns together, that disputes the fact that they not only know each other but would pose for that picture," O'Brien

said.

According to O'Brien, people cannot resist the urge to talk.

"Sometimes you wonder what people are doing when they post either comments or photos on the Web page that shows them with drugs, guns and money, and you wonder what they're thinking when they do that," O'Brien said.

Police typically need search warrants signed by judges to access Facebook accounts, Kocot reported.

Slithering ssstupidity

Vanessa Marsh | 23rd January 2012

A CLUMSY crook who made off with a snake from a local reptile park didn't slither far after a forensic investigator found he not only left his phone at the crime scene, he posted a photo of the stolen animal on Facebook.

About 5.30am yesterday, Snakes Downunder Reptile Park owner Ian Jenkins found his business had been broken into and Titch, a young pygmy python, had been stolen from her enclosure.

"She might be worth a couple of thousand dollars but that's not what I was worried about," he said.

"It's her safety we were worried about.

"Because she's so small, she gains heat very quickly so she could overheat and die."

Mr Jenkins was quick to call the police, who sent out a forensic officer to examine the scene.

"Our very alert scenes of crime officer, who attended the scene, located the offender's phone in a matter of seconds," Bundaberg police Sergeant Mike McLellan said.

"He found it in the dirt of the snake pit and in a few seconds, all was revealed."

Sgt McLellan said the phone, along with a Facebook photo showing the snake, led officers right to the door of a 14-year-old boy who, at this stage, has not been charged over the offence.

Mr Jenkins said he was thrilled Titch had been returned.

"It's a bit of a wake-up call to us to look at upgrading security," he said.

"We don't want anything like this to happen again."

Mr Jenkins said it appeared the offender knew what he was looking for, heading right to Titch's enclosure and taking no other snakes.

Facebook pictures lead to stolen ring

Published: Dec. 29, 2011 at 12:08 PM

BURLINGTON, Vt., Dec. 29 (UPI) -- Police in Vermont said a man was arrested for stealing an engagement ring after his fiancée posted pictures of the item on Facebook.

Burlington police said three people contacted police Tuesday to report seeing a ring matching the description of the one taken Monday from Zales Jewelry on Church Street in photographs on Amber Lafountain's Facebook page, the Burlington Free Press reported Thursday.

Lafountain said the ring was given to her by fiancé Ryan Jarvis, 25, who admitted to police he ran off with the \$3,199 ring Monday after determining he would not be able to afford it.

"He reported that he considered financing options, but concluded that he would be unable to afford the ring he wanted," Officer Jesse Stewart wrote in a sworn affidavit. "He reported that he then ran out of the store with the ring. He advised he knew it was a stupid thing to do."

Jarvis pleaded not guilty Wednesday to one felony count of retail theft.

Upon Further Review

February 07, 2012

A Publication of the Philadelphia Bar Association

The Foundations of Foundations: Admission of Documentary Exhibits into Evidence at Trial

Steven E. Bizar, Esq. on 12/05/2008

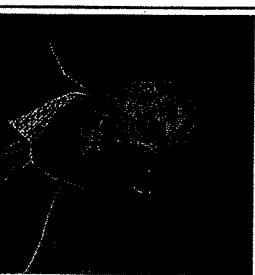


Recent news articles and speeches have decried the vanishing civil jury trial, particularly in cases involving business disputes. Perhaps equally alarming is the related phenomenon that scores of litigators apparently are not developing the basic techniques necessary to try cases. One example is the lost art of “foundating” a document so it can be admitted into evidence at trial.

We have attended, taken and defended countless depositions and yet are always surprised when lawyers lack even the most basic understanding of how to lay a foundation for the admission of documents into evidence at trial. There are many possible explanations: inexperience; poor preparation; over-reliance on the assumption that the parties will stipulate to the admissibility of evidence; laziness. Some of these explanations are benign, others not, but none reflect well on our profession. Working with documentary evidence and ensuring that it is available for use at trial is a basic skill that every civil trial lawyer should possess, regardless of whether the case actually proceeds to trial. It is not difficult but does require advance planning and an understanding of the rules and process.

We are not suggesting that shortcuts – such as stipulations – are not appropriate. A stipulation that a document is authentic and admissible as a business record is valuable if it can be obtained before it is too late (i.e., before the discovery cut-off and summary judgment briefing). Similarly, we are not suggesting that written discovery has no place in the process. We have both used and responded to Requests for Admissions that aim to resolve authentication issues and secure admissions that certain documents are admissible as business records. Like stipulations, admissions (if they can be obtained) save time and trouble at trial and be used with adverse parties or even co-defendants (obviously, if a co-defendant settles, your plan to introduce its documents at trial through its witnesses falls apart; an admission can resolve this dilemma). Problems occur, however, when a stipulation is not available (for example, if opposing counsel will not agree to it), or the document you need to be able to use comes from a non-party, in which case Requests for Admissions are not appropriate (Fed. R. Civ. P. 36 applies only to parties), or the witness you were counting on to testify at trial about the authenticity of the document is outside the reach of the court’s

About The Author



Buchanan Ingersoll & Rooney, PC

Contact Steven E. Bizar, Esq.

More by Steven E. Bizar, Esq. »

subpoena power and refuses to appear and testify voluntarily at trial. It is vital that lawyers anticipate these real possibilities and take steps to properly lay the foundation for the document's admission during a deposition so it may later be used at trial.

Most evidence requires some predicate of foundation in order to be admitted. Laying an evidentiary foundation is usually not a burdensome task and, ordinarily, there is no need to elicit extensive testimony to do so. As a preliminary matter, the witness you are using to lay a foundation must be competent to testify about the exhibit; in the case of a business record, the witness should be the custodian of records or some other qualified witness. Next, as a "condition precedent to admissibility," a document must be authenticated or identified to show that it is what it purports to be. See Fed. R. Evid. 901(a); see also Fed. R. Evid. 901(b) (containing illustrative examples of ways to authenticate documents); cf. Fed. R. Evid. 902 (listing self-authenticating documents). This liberal standard favors the admission of evidence. Even if the document is shown to be authentic, it does not necessarily follow that it will be admissible; the document must still satisfy the relevancy requirements and the hearsay rules. Therefore, a lawyer also needs to demonstrate that the document is not hearsay or falls within a hearsay exception (e.g., it is a recorded recollection or business record). See Fed. R. Evid. 801-804.

For example, a document created by your client's opponent may come into evidence as an admission by a party opponent. See Fed. R. Evid. 801(d)(2). So, at the deposition, the questioning should seek to establish that the document is what it appears to be – e.g., an internal e-mail in which top executives of the adverse party admit that they are in breach of their contract with your client. Similarly, lawyers can establish that a document is admissible as a business record – the most common hearsay exception in business litigation – by asking the appropriate witness a simple series of questions at the deposition to establish (i) that the witness is a custodian of the document or otherwise qualified to discuss it (e.g., because she wrote it, received it, approved it, acted on it, etc.), (ii) that it was created at or near the time of the events it discusses, (iii) that it was created by, or from information transmitted by, someone with knowledge of the events in question (double or triple hearsay does not become admissible merely because it is included in a "business record"), and (iv) that making the document was a regular part of the witness's or the witness's colleague's business and keeping it was a regular part of the company's business. See Fed. R. Evid. 803(6).

Even after an attorney lays the foundation for evidence, the document is subject to other admissibility objections, as permitted by Federal Rules of Evidence. See, e.g., Fed. R. Evid. 403 (stating that evidence may be excluded if its probative value is outweighed by the danger of unfair prejudice). Once a party makes such an objection, the court must make a ruling as to the admissibility of the evidence. See Fed. R. Evid. 104. Thus, laying a foundation does not guarantee the admissibility of an exhibit, but it is an essential step that every prudent trial lawyer should be able to do skillfully and effortlessly – and which, with a little advance planning and an understanding of the rules, they can.

Resources

STEVEN LUBET, *MODERN TRIAL ADVOCACY: ANALYSIS AND PRACTICE* 307-82 (3rd ed. 2004).

JAMES W. MCELHANEY, *MCELHANEY'S TRIAL NOTEBOOK* 337-89 (4th ed. 2005)

PAUL MARK SANDLER AND JAMES K. ARCHIBALD, MODEL WITNESS EXAMINATIONS (1st ed. 1997)

5 STEPHEN A. SALTZBURG, ET AL., FEDERAL RULES OF EVIDENCE MANUAL §§ 901-02 (9th ed. 2006).

Philadelphia Bar Association

1101 Market St., Philadelphia, PA 19107

(215) 238-6300 | philabar.org

Authenticating E-Mail Discovery as Evidence

With the recent passage of the amendments to the Federal Rules of Civil Procedure, the legal press has been filled with articles containing e-discovery advice. At some point, "e-discovery" will need to be converted into "e-evidence" for the purposes of summary judgment or trial. When you're faced with having spent your clients' time and money to both produce e-discovery and mine your opponents' e-discovery to find the "smoking gun," it's critical to ensure you can get those e-mails into evidence — or keep them out.

Many practitioners think that e-mails are like business letters and will be admitted into evidence just as easily. E-mails, however, may be more prone to problems of authenticity and hearsay than traditional written documents. People often write e-mails casually, dashing off comments with an informality they'd never use with a letter. Little care is given to grammar and context. Their signature or even their name may be omitted. Authenticating an e-mail presents issues not faced with a traditional letter with its formal letterhead, paragraph structure and signature block. Additionally, e-mails are arguably more susceptible to after-the-fact alteration.

Most e-mail systems, for instance, allow a person forwarding an e-mail to edit the message being forwarded. Such alteration wouldn't be discernible to the recipient. E-mails are also more prone to a kind of hearsay-within-hearsay problem: an "e-mail chain" attaches to an e-mail every e-mail that came before it in a discussion. It isn't enough to get the most recent e-mail into evidence when that e-mail attaches a string of previous e-mails. All of the prior e-mails may need to be separately authenticated and found admissible.

Given the dramatic shift toward the use of e-mails in business communications, courts and practitioners are likely to encounter issues of e-mail evidence more frequently than in the past. Are e-mails so different from traditional written documents that the rules of evidence are out of date? We think that there are practical ways to employ the rules of evidence to confront the special admissibility problems posed by e-mails.

AUTHENTICATION

In order to ensure that an e-mail will be admitted into evidence, a proper foundation for its authenticity must be laid.

Authentication is necessary not only at trial but also at the summary judgment stage.

Although challenges to the admissibility of evidence are not always raised in response to summary judgment motions, a lawyer should be prepared to submit evidence in the form of affidavits to support the authenticity of any e-mail that he or she intends to introduce. In several instances, courts have excluded e-mails at the time of dispositive motion — not because the e-mails were clearly inauthentic, but because evidence wasn't submitted to support their authenticity in the face of a challenge. One such case is the Western District of Pennsylvania's *Bouriez v. Carnegie Mellon University*.

Similarly, a lawyer may need to depose a witness to establish the authenticity of an e-mail, based on the witness' personal knowledge, or to have that witness available at trial. Stipulations and requests for admissions can eliminate authentication issues or narrow the scope of those e-mails that will be problematic. In federal court, the parties may choose at their Rule 26(f) conference to agree to a process for stipulating to the authenticity of e-mails each party produces during discovery to avoid unnecessary expense.

The bar for establishing authenticity is not high under Federal Rule of Evidence 901. In the 3rd U.S. Circuit Court of Appeals, a court need only be able to legitimately infer that a document is genuine to find it to be "authentic." Deeper questions concerning trustworthiness might go to the weight of the evidence. In *U.S. v. Safavian*, faced with a mountain of e-mails, the court refused to require detailed authentication.

Some e-mails can be self-authenticated under Rule 902(7). Business labels, including signature blocks, that evidence the company from which an e-mail was sent, or even the name of a company in an e-mail address, might be sufficient proof of authenticity on their own. Other circumstances, such as the distinctive characteristics of an author's e-mail address or the subject matter and style of the e-mail itself, may also be sufficient to establish authenticity.

An e-mail often has attached to it the e-mail or series of e-mails to which it is responding, creating an e-mail "chain," also known as a "string" or "thread." Some courts have found that each e-mail in a chain is a separate communication, subject to separate authentication and admissibility requirements. A lawyer should thus be prepared to authenticate every step of a chain.

The Pennsylvania Superior Court, however, has noted that uncertainties of authenticity for e-mails are the same as for traditional written documents: "A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationery [sic] can be copied or stolen," according to *In re F.P.* The court therefore rejected the notion that e-mail is inherently more unreliable than traditional written documents, as well as the argument that e-mail cannot be properly authenticated within the existing framework of Pennsylvania law.

HEARSAY

The second major hurdle for getting an e-mail into evidence is the hearsay rule. By definition, hearsay is an out-of-court statement "offered in evidence to prove the matter asserted." The first way, therefore, to overcome a hearsay challenge to the admission of an e-mail is to claim that it's not hearsay at all.

An e-mail that is an admission by a party-opponent is "not hearsay." If your opponent is an individual, this is a simple test. In the corporate setting, however, damaging admissions may be authored by lower-level employees who do not have the authority to be making such statements. In order for the e-mail to qualify as a party admission, the author needs not only to be acting in the scope of his or her employment but also to have the proper authority.

Party-opponent admissions would also include statements by “a party’s agent” concerning matters within the scope of the agency, i.e., “vicarious admissions.” In addition, if your opponent’s e-mails contain statements of others without reservation, e.g., when a party forwarded e-mails received from others, the e-mails may be introduced in evidence as “adoptive admissions,” according to Safavian. This kind of statement has indicia of reliability because “the party has manifested an adoption or belief in its truth.”

Another way to overcome a hearsay challenge is to fit the e-mail into one of the exceptions to the hearsay rule. These exceptions are permitted because their context makes them likely to be reliable.

Many practitioners would consider e-mails as classic examples of business records for corporate entities that routinely use e-mail for both internal and external communication. Under Federal Rule of Evidence 803(6), however, only “if it was the regular practice of that business activity” to make that record can a document come into evidence under the exception. An e-mail might fit this “business records” exception if the company — not just the individual, but the company itself — has a reliable practice of sending, receiving and storing that kind of e-mail. A company might have that kind of practice if it takes and records purchase orders via e-mail. Notably, an e-mail that fits into the “business records” exception may also be self-authenticating, under Rule 902(11), if its authenticity is supported by an affidavit.

Many e-mails, however, do not meet the “business records” exception because they are merely chatter, statements that are made casually and not as a matter of obligation or even routine. An e-mail sent at an employee’s sole discretion is not likely to have the necessary indicia of reliability and trustworthiness to be admitted as a “business record.” If an employee sends off a quick e-mail to a colleague commenting on the substance of a meeting with a business partner, it may not be admissible. By contrast, minutes of the same meeting kept by the same employee and circulated to all in attendance, in e-mail form, at the request of management could qualify under the “business records” exception. Although there is not yet a well-established line of cases on this issue, courts appear concerned that if they allow e-mails into evidence as “business records” too easily, people will begin to use the convenience of e-mails to write self-serving internal communications.

With the advent of handheld devices as well as the ubiquity of laptop computers, e-mails may actually be admitted into evidence on the basis of “present sense impressions,” or even as “excited utterances,” as in *Lorraine*. People are often using e-mail to comment on events as they are transpiring, even during meetings. If one can show that an e-mail was written while perceiving an event or immediately thereafter, or while under the stress caused by a startling event, it might meet the “present sense impression” or “excited utterance” standards of rules 803(1) and 803(2).

Of course, these standards are difficult to meet because contemporaneousness or near-immediacy is necessary. An e-mail might still meet the “present sense impression” standard if written 10 minutes after an event, but many e-mails are written hours or days later.

Just as with authentication, one should be prepared to argue for the admissibility, under the hearsay exceptions, of every e-mail in an e-mail chain, as in *New York v. Microsoft Corp.* One should also be

aware, as with authentication, that evidence that is clearly inadmissible at trial cannot be considered by a court on summary judgment.

Although Rule 56 does not require an unequivocal ruling that an e-mail will be admissible at trial for a court to consider it on summary judgment, one should be prepared to support its admissibility with an affidavit.

The special problems posed by e-mails do not change the rules of impeachment. A lawyer's ability to cross-examine a witness with a prior inconsistent statement does not change merely because the statement is contained in an e-mail.

BE PROACTIVE

The admissibility problems related to e-mail extend to other forms of electronically stored information, too. Text messages, instant messaging, chat rooms or "team rooms" (in which all materials concerning a project are preserved electronically for the entire project team to access) all present unique evidentiary challenges.

Practitioners need to be proactive in their efforts to ensure that key pieces of evidence can be admitted at trial. From the time of the initial review of documents through discovery, lawyers need to focus on how to get in or keep out such evidence.

Beatrice O'Donnell is a senior partner in the trial practice group of Duane Morris. She practices in the areas of product and professional liability, as well as commercial and insurance litigation. O'Donnell has tried to verdict more than 80 major civil jury trials in both state and federal courts, and has tried hundreds of arbitrations and mediations. She has been both national and regional coordinating counsel for a number of pharmaceutical and other clients facing mass tort litigation. Thomas A. Lincoln is an associate with the trial practice group of the firm.

E-Discovery Advisory

From the Buchanan Ingersoll & Rooney E-Discovery Team

Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

June 2011

Destruction of Electronic Evidence, Discovery Misconduct Lead to \$1 Million Fine, Default Judgment

By Rajesh C. Noronha

In a February 23, 2011 opinion and order, Judge Sharon Johnson Coleman granted the motion of Trading Technologies International, Inc. ("Defendant") for default judgment and monetary sanctions, based on misconduct by Rosenthal Collins Group, LLC ("Plaintiff") and its counsel with respect to the preservation and production of electronic evidence. *Rosenthal Collins Group, LLC v. Trading Technologies International, Inc.*, No. 05-C-4088, 2011 WL 722467 (N.D. Ill. Fed. 23, 2011) (hereinafter, "*Trading Techs.*").

Finding that "both [Plaintiff] and its counsel acted willfully in bad faith by engaging in conduct that resulted in deception of both the opposing party and the Court, the destruction of relevant evidence, the waste of judicial resources, and the undermining of the judicial process," the Court imposed a sanction on Plaintiff of \$1,000,000 and default judgment against Plaintiff. In addition, "[f]or their part in presenting misleading, false information, materially altered evidence, and willful non-compliance with the Court's orders," Plaintiff's counsel was ordered to pay the costs and attorneys fees related to litigating the motion.

In finding that Plaintiff and its counsel had committed misconduct which warranted the sanction of dismissal, the Court noted the following:

1. **Evidence tampering; Lack of candor.** Plaintiff's consultant admitted to altering and overwriting source code to make it appear that it had been last modified much earlier, which was of critical importance to the claims in the case. Plaintiff and its counsel had denied Defendant's allegations that the dates had been altered, characterizing those allegations as "libelous," "audacious," and an "Oliver Stone-esque" conspiracy theory. The Court held:

[Plaintiff] and its counsel had an affirmative duty to make sure that the metadata was accurate in light of their reliance on the source code. . . . Instead of inquiring further into the matter, [Plaintiff] opted to stay the course and continue to deny any wrongdoing.

2. **"Wiping" electronic media.** Media which purportedly contained original source code had been "wiped" (erased and rendered unrecoverable) by Plaintiff's consultant before being produced to Defendant. Additional media purported to contain original source code was "wiped" only hours before it was inspected by Defendant's counsel.
3. **Spoilation of evidence previously ordered to be produced.** Forensic analysis indicated that "virtually every piece of media ordered produced by the Court in May 2007 and July 2008 was wiped, altered, or destroyed after those orders were entered."

4. **Gross negligence or recklessness.** While Plaintiff claimed that it had no knowledge of the misconduct of its consultant and argued that it should not be held responsible for his actions, the Court determined that Plaintiff was not immune from sanctions, stating:

The imposition of sanctions, however, does not require actual knowledge, but gross negligence or recklessness, i.e., [Plaintiff] knew or should have known. . . . Even if this Court were to accept that [Plaintiff] had no actual knowledge of the evidence destruction and modification that occurred, [Plaintiff's] conduct still warrants the imposition of a default judgment.

5. **Failure to preserve relevant evidence; Failure to comply with Court orders on discovery.** The failure of Plaintiff to follow the orders of the Court and preserve electronic evidence allowed for spoliation to occur. As the Court reasoned:

[Plaintiff] and its counsel had a duty to preserve the evidence, which they could have done by taking physical possession of, or obtaining forensic images, of the evidence. It appears that [Plaintiff] took no steps after the first order to collect the evidence to ensure its preservation. . . . Parties to a lawsuit have a duty to preserve admissible evidence as well as evidence that is discoverable because it is "reasonably calculated to lead to the discovery of admissible evidence." (citations omitted).

6. **Failure to take reasonable measures to ensure preservation of evidence.** Plaintiff claimed that it told its consultant to preserve everything related to the software. However, the Court reasoned that:

[I]t is evident to this Court, and should have been equally apparent to counsel for [Plaintiff], who actually interacted with [Plaintiff's consultant], that [Plaintiff's consultant's] understanding of what "preserve" means was dramatically different from what is intended by that word for litigation purposes. Moreover, simply telling [Plaintiff's consultant] to preserve everything related to the [software], does not strike this Court as a reasonable means of ensuring preservation of evidence material to this lawsuit, especially after the Court had specifically ordered certain pieces of equipment to be produced.

7. **Responsibility for agent's actions.** Plaintiff's consultant was "under [Plaintiff's] control and was its paid agent," such that Plaintiff was bound by his behavior and actions.
8. **Failure to take reasonable measures to ensure completeness and accuracy of disclosures.** Sanctions were required for the failure of Plaintiff to act reasonably in making disclosures in discovery. As the Court stated:

"Under Rule 26(g), a court must impose sanctions against the party, its counsel, or both, when the party fails to meet its disclosure obligations under Rule 26. The completeness and accuracy of these disclosures must be certified by an attorney of record. This certification requirement includes an obligation to conduct a reasonable inquiry into the disclosures. (citations omitted).

A motion for reconsideration and clarification of the sanctions order was filed by Plaintiff. The Court denied the motion, stating: "This Court's order entering default judgment and sanctions was tailored to the misconduct at issue. [Plaintiff] attempts to minimize the implications of its misconduct, treating the matter as a simple issue of discovery compliance. This Court reminds [Plaintiff] that the conduct at issue was far more insidious, constituting an attempt to commit a fraud on the Court by fabricating evidence of prior art and engaging in systematic spoliation of evidence." Memorandum Opinion and Order, June 1, 2011, Doc. No. 489 at p. 2. As the Court reiterated, "The sanctions imposed were proportionate to the wrong, which this Court found to be willful and egregious." *Id.* at p. 4.

The *Trading Techs.* case provides various lessons for parties and counsel engaged in litigation, especially when electronic discovery is involved. The key take-aways from the case are:

1. Candor with the Court and other parties must be maintained at all times.
2. Reasonable efforts to ensure the completeness and accuracy of information disclosed in discovery is required under Fed. R. Civ. P. 26.
3. It is important to preserve electronic evidence properly, ensuring that such evidence is not altered or destroyed. "Litigation holds" should be put in place as soon as possible to ensure that such practices as routine electronic file purges or scheduled hard copy shredding do not destroy relevant evidence. Ensure that a party and its agents, including consultants, are aware of the duty to preserve all relevant evidence. Actual knowledge of discovery misconduct is not necessary for sanctions to be imposed on a party or its counsel, as gross negligence or recklessness (i.e., knew or should have known) can be enough.
4. Do not erase, alter or destroy even questionably relevant evidence.
5. Never falsify documents. While this, of course, goes without saying, it must be underscored in an age of electronic discovery. As seen in *Trading Techs.*, an electronic trail may remain as a result of any alteration to an electronic file, and this trail may be readily apparent or can be uncovered through forensics.
6. Make all reasonable efforts to timely comply with discovery requests, including making arrangements for discovery of electronic files and media.
7. Comply with Court orders regarding discovery, both in terms of scope and timing. As the Court indicated in *Trading Techs.*, the failure of the Plaintiff to adhere to Court orders on discovery allowed spoliation of evidence to incur and, eventually, sanctions to be imposed.